普通高等教育"十一五"国家级规划教材

高等院校信息安全专业系列教材

教育部高等学校信息安全专业教学指导委员会
中国计算机学会教育专业委员会
共同指导

顾问委员会主任：沈昌祥　编委会主任：肖国镇

网络安全（第2版）

胡道元　闵京华　编著

方滨兴　审

http://www.tup.com.cn

Information Security

根据教育部高等学校信息安全专业教学指导委员会编制的《高等学校信息安全专业指导性专业规范》组织编写

清华大学出版社

普通高等教育"十一五"国家级规划教材
高等院校信息安全专业系列教材

网络安全（第2版）

胡道元　闵京华　编著　方滨兴　审

清华大学出版社
北　京

内 容 简 介

网络安全是在分布网络环境中,对信息载体(处理载体、存储载体、传输载体)和信息的处理、传输、存储、访问提供安全保护,以防止数据、信息内容或能力被非授权使用、篡改或拒绝服务。

全书共分4篇20章,全面讲述网络安全的基础知识(网络安全的入门和基础),Internet安全体系结构(依照Internet层次结构的原则,对不同类型的攻击实施不同层的保护),网络安全技术(防火墙、VPN、IPSec、黑客技术、漏洞扫描、入侵检测、恶意代码与计算机病毒的防治、系统平台及应用安全)及网络安全工程(网络安全设计、管理和评估)。

本书内容翔实,结构合理,概念清楚,语言精练,实用性强,易于教学。

本书可作为信息安全、计算机和通信等专业本科生和研究生的教科书,也可供从事相关专业的教学、科研和工程人员参考。

图书在版编目(CIP)数据

网络安全/胡道元,闵京华编著.—2版.—北京:清华大学出版社,2008.10
(高等院校信息安全专业系列教材)
ISBN 978-7-302-17963-4

Ⅰ.网…　Ⅱ.①胡…②闵…　Ⅲ.计算机网络-安全技术-高等学校-教材
Ⅳ.TP393.08

中国版本图书馆CIP数据核字(2008)第093142号

责任编辑: 张　民
责任校对: 白　蕾
责任印制: 何　芊

出版发行: 清华大学出版社　　**地　址:** 北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　编:** 100084
社 总 机: 010-62770175　　**邮　购:** 010-62786544
投稿与读者服务: 010-62776969,c-service@tup.tsinghua.edu.cn
质 量 反 馈: 010-62772015,zhiliang@tup.tsinghua.edu.cn
印 刷 者: 北京密云胶印厂
装 订 者: 三河市金元印装有限公司
经　销: 全国新华书店
开　本: 185×230　　**印　张:** 28　　**字　数:** 655千字
版　次: 　年　月第2版　　**印　次:** 　年　月第　次印刷
印　数: 1～5000
定　价: 43.00元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。联系电话:010-62770177转3103　　产品编号: -

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教

材中,以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍,同时也欢迎广大读者对本系列教材提出宝贵意见,以便我们对本系列教材的组织、编写与出版工作不断改进,为我国信息安全专业的教材建设与人才培养做出更大的贡献。

"高等院校信息安全专业系列教材"已于2006年年初正式列入普通高等教育"十一五"国家级教材规划(见教高[2006]9号文件《教育部关于印发普通高等教育"十一五"国家级教材规划选题的通知》)。我们会严把出版环节,保证规划教材的编校和印刷质量,按时完成出版任务。

2007年6月,教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办,清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。"高等院校信息安全专业系列教材"将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下,进一步体现科学性、系统性和新颖性,及时反映教学改革和课程建设的新成果,并随着我国信息安全学科的发展不断修订和完善。

我们的E-mail地址:zhangm@tup.tsinghua.edu.cn;联系人:张民。

清华大学出版社

第2版前言

网络安全，尤其是 Internet 安全正面临着严重的挑战，一方面是Internet规模的扩大和关键应用的激增，因而对网络安全的需求很高；另一方面是网络安全攻击的持续增加、安全漏洞的增长，使实施网络安全的难度大大增加。

从网络安全体系结构的观点看，不同类型的漏洞、攻击、威胁存在于网络的不同层次。层次的方案深入研究网络环境的各种技术及每一层次的每种技术的复杂性。第 2 版充实了 Internet 安全体系结构的内容，更新了一些网络安全技术及网络安全管理技术。具体有以下几点：

(1) 第 1 章增加了一节网络安全挑战，论述了当前网络安全形势。

(2) 第 5 章改为安全体系结构，论述了系统安全体系结构、OSI 安全体系结构及网络安全体系结构。

(3) 第 2 篇改为 Internet 安全体系结构，论述了依照层次结构的原则，对不同类型的攻击实施不同层的保护。

(4) 更新了第 11～13 章及第 15 章部分内容。

(5) 参照新公布的 ISO/IEC FDIS 18028 重新编写了第 19 章网络安全管理。

本书共分 4 篇 20 章。第 1 篇为网络安全基础知识，共 5 章，是网络安全的入门和基础知识。第 2 篇为 Internet 安全体系结构，共 2 章，讲述依照Internet层次结构的原则，对不同类型的攻击实施不同层的保护。第 3 篇为网络安全技术，共 9 章，讲述各种网络安全技术。第 4 篇为网络安全工程，共 4 章，分别讲述网络安全设计、管理和评估。

每章开始列出本章要点，每章最后一节给出小结，概要地总结本章的要点。每章结尾附有习题，帮助读者复习。

本书可作为信息安全、计算机和通信等专业本科生和研究生的教科书，也可供从事相关专业的教学、科研和工程人员参考。

本书由胡道元教授主编并编著了第 1～7 章、第 17、18 和 20 章，闵京华博士编著了第 14、16和 19 章，朱卫国编著了第 15 章，陆新宇、邢羽嘉编著了第 11～13 章。黄新民、刘旺泉编著了第 8～10 章。

参与第 2 版编写的有胡道元(第 1 章、第 5～7 章)、闵京华(第 19 章)、朱卫国(第15 章)、陆新宇(第 11～13 章)。

胡道元于北京

第1版前言

我们生存的世界并不安宁，人们渴望有一个安全、和平的生存空间，随着信息技术的发展，特别是网络的发展，人们的诸多活动越来越多地依赖于网络空间，然而，网络空间并非总是安全的。

当前我国的网络安全正面临着严峻的挑战。一方面，随着电子政务工程的启动、电子商务的开展以及国家关键基础设施的网络化，网络安全的需求更加严格和迫切。另一方面，黑客攻击、病毒传播以及形形色色的网络攻击日益增加，网络安全防线十分脆弱。

网络安全是在分布网络环境中，对信息载体(处理载体、存储载体、传输载体)和信息的处理、传输、存储、访问提供安全保护，以防止数据、信息内容或能力被非授权使用、篡改或拒绝服务。

从本质上讲，安全就是风险管理，风险是构成安全基础的基本观念。风险是丢失需要保护的资产的可能性，是威胁和漏洞的综合结果。没有漏洞的威胁就没有风险，而没有威胁的漏洞也没有风险。

“网络安全”是信息安全专业的主要专业课，学生应从以下三个方面掌握网络安全的基本原理、主要技术以及解决方案：

(1) 网络安全体系结构

由开放系统互连模型和Internet层次体系结构决定了网络安全体系结构的层次模型。网络安全体系结构描述网络信息体系结构在满足安全需求方面各基本元素之间的关系，反映信息系统安全需求和网络体系结构的共性。并由此派生了相应的网络安全协议、技术和标准。

(2) 网络安全技术

单一的网络安全技术和网络安全产品无法解决网络安全的全部问题。应根据应用需求和安全策略，综合运用各种网络安全技术，包括防火墙、VPN、IPSec、黑客技术、漏洞扫描、入侵检测、恶意代码与计算机病毒的防治、系统平台安全及应用安全等。

(3) 网络安全工程

对网络安全进行的综合处理，要从体系结构的角度，用系统工程的方法，贯穿网络安全设计、开发、部署、运行、管理和评估的全过程。

本书共分4篇20章。第1篇为网络安全基础知识，共5章，是网络安全的入门和基础。第2篇为网络安全体系结构，共2章，讲述开放系统互连安

全体系结构和 Internet 安全体系结构。第 3 篇为网络安全技术,共 9 章,讲述各种网络安全技术。第 4 篇为网络安全工程,共 4 章,分别讲述网络安全设计、管理、评估。

每章开始列出本章要点,最后给出小结,概要地总结本章的要点。每章结尾附有习题,帮助读者复习。

本书可作为信息安全、计算机、通信等专业本科生、硕士研究生的教科书,也可供从事相关专业的教学、科研和工程人员参考。

本书由胡道元教授主编并编著了第 1 章~第 7 章、第 17、第 18 和第 20 章,闵京华博士编著了第 14、第 16 和第 19 章,朱卫国编著了第 15 章,邵忠岿、黄新民、刘旺泉、陆新宇、邢羽嘉分别编著了第 8 章~第 13 章。赵青为书稿的编排、打印做了大量的工作。闵京华博士做了全书的最后校订工作。

作　者

目 录

第1篇　网络安全基础知识

第2篇 Internet 安全体系结构

第3篇 网络安全技术

第 4 篇 网络安全工程

第 1 篇
网络安全基础知识

第1章 引　论

本章要点：

- 分布网络环境下的安全；
- 网络安全的定义；
- 网络安全的基本属性；
- 网络安全的层次结构；
- 网络安全模型；
- 网络安全挑战；
- 密码基本概念。

1.1 网络安全概述

1.1.1 网络安全的概念

首先从信息安全的一般性定义来阐述。Merriam-Webster 在线词典(www. m-w. com)对信息这个词作了广泛而精确的阐述：信息是从调查、研究和教育获得的知识，是情报、新闻、事实、数据，是代表数据的信号或字符，是代表物质的或精神的经验的消息、经验数据、图片。在线词典对安全这个词的阐述：安全是避免危险、恐惧、忧虑的度量和状态。

将上述信息和安全两个词的定义合并起来，可给出信息安全的一般性定义：信息安全是防止对知识、事实、数据或能力非授权使用、误用、篡改或拒绝使用所采取的措施(量度)。

从信息安全的一般性定义，进一步引出本书的主题——网络安全的定义。为此先给出计算机网络的定义。计算机网络是地理上分散的多台自主计算机互联的集合。自主计算机这一概念排除了网络系统中主从关系的可能性。互联必须遵循约定的通信协议，由通信设备、通信链路及网络软件实现。计算机网络可实现信息交互、资源共享、协同工作及在线处理等功能。为了保证安全，需要自主计算机的安全；互联的安全，即用以实现互联的通信设备、通信链路、网络软件、网络协议的安全；各种网络应用和服务的安全。总之，我们强调的是在分布网络环境下的安全。

计算机网络的通信采用分组交换方式，分组从源站出发通过路由器在网络中传送，最终到达目的站接收。目前广泛采用 TCP/IP 协议，所用的地址即 IP 地址。不难看出，这种基于 IP 的 Internet 有很多不安全的问题。下面分别予以阐述。

1. IP 安全

在 Internet 中，当信息分组在路由器间传递时，对任何人都是开放的，路由器仅仅搜集信息分组中的目的地址，但不能防止其内容被窥视。当黑客企图攻击网络前，他必须设法登录到接入网上的某些计算机，观察流动的数据分组，找到他感兴趣的内容。如果他接近并进入到某公司的一台外围计算机，他就极有可能监视进出这一系统的所有数据。

黑客最感兴趣的是包含口令的数据分组。口令窃听十分容易，而且是 Internet 最常见的攻击。黑客要安装一个用于窃取用户名和口令的分组窃听程序，这些程序可帮助黑客窃取每次登录会话信息中的头几十个字节，并保存起来。这些字节包括用户名和口令，口令通常是加密的，需要对日常口令进行破解，用破解的口令登录其他计算机。

除了网络窃听外，另一种攻击称为网络主动攻击，即在通信系统中主动插入和删除信息分组。因为网络通信是基于分组的，分组的传输经过不同的路径最后在目的地组装，黑客利用现有的通信通道，任意地插入信息分组。这叫作 IP 欺骗，实现起来很容易，信息分组中包括源地址和目的地址，但黑客可对其进行修改。黑客创建一个看似发自某一站点的信息分组，当 Internet 上的计算机看到一个分组来自于它所信任的计算机时，它就会认为对方发出的信息分组也是可信的。黑客就是利用这些信任关系攻入某台计算机，发送一个来自被信任计算机的伪造信息分组，以使目的计算机信任并接收。

另一种主动攻击称为路由攻击，这时攻击者告诉网上的两个结点，它们之间最近的传输线路就是经过他这台计算机的路径，这就使该台计算机的侦听变得更容易。

要解决这些问题，在理论上显得较容易，但实现起来却不尽然。如果把信息分组加密，传输过程中就不易解读；如果对数据分组进行验证，就可发觉插入了伪造信息分组或删除了某个信息分组。对 Internet 上信息分组的加密有多种方法，例如，能对一台计算机的用户经网络登录另一台计算机的连接进行加密并验证的方法，可以加密验证 Internet 上的 Web 数据流的方法，能加密验证 IP 通道上所有信息的方法等。

2. DNS 安全

Internet 对每台计算机的命名方案称为域名系统(DNS)。域名和 IP 地址是一一对应的，域名易于记忆，用得更普遍。当用户要和 Internet 上某台计算机交换信息时，只需使用域名，网络会自动转换成 IP 地址，找到该台计算机。同时域名也用于建立 URL 地址和 E-mail 地址。

DNS 有两个概念上独立的要点：一个是抽象的，即指明名字语法和名字的授权管理规则；另一个是具体的，即指明一个分布计算系统的实现，它能高效地将名字映射到地址。

域名方案应包括一个高效、可靠、通用的分布系统，实现名字对地址的映射。分布的系统是指由分布在多个网点的一组服务器协同操作解决映射问题。高效的系统是指大多数名字映射在本地操作，只有少数名字映射需要在 Internet 上通信。通用的系统是指它不使用机器名。可靠的系统是指单台计算机的故障不会影响系统的正常运行。

DNS 系统并不总是安全的。当一台计算机向 DNS 服务器发出查询请求，并收到回应时，它认为这一回应是正确的，DNS 服务器也是真实的。其实 DNS 服务器并非总是真

实的，也有可能存在欺骗。计算机收到的 DNS 服务器的应答可能并不是来自 DNS 服务器，而是来自其他地方的虚假回应。如果黑客改动了 DNS 表，即改动了从域名到 IP 地址（或反之）的转换数据，计算机也会默认接受。

这种黑客攻击的结果是使一台计算机相信他的请求回应来自另一台可置信计算机，因为通过改变 DNS 表，使黑客计算机的 IP 地址成为可信任的 IP 地址。网络攻击者会劫持并改变一个网络连接，攻击者可能做各种类似的操作。DNS 服务器会执行修改过程，如果一台 DNS 服务器的记录发生了变化，它就会通知另一台 DNS 服务器，以致这种改动将在整个 Internet 上繁殖。这与闯入某 Web 站点建立主页页面的性质不同，黑客通过操纵 DNS 记录合法访问系统，并导向他们制作的假主页。他们并未攻击 DNS 服务器，而是攻击 DNS 服务器上的信息流。

DNS 安全问题看来很严重，且难以解决。密码学和鉴别方法可能是较好的解决途径，因为计算机不会贸然相信那些声称是来自 DNS 服务器的信息。人们正在研究 DNS 系统的安全版本，但尚需时日。

3. 拒绝服务（DoS）攻击

（1）发送 SYN 信息分组

第一例引起公众关注的袭击 Internet 主机的拒绝服务攻击发生于 1996 年 9 月，一名黑客攻击了纽约一家 ISP（公共访问网络）公司 Panix 的一台计算机。攻击的方式是由一台远程计算机向 Panix 发问候语，Panix 计算机接收并响应，之后远程计算机继续与之对话。攻击者操纵远程计算机的返回地址，并以每秒 50 个 SYN 信息分组向 Panix 大量发送，Panix 难以负担如此大量的信息，结果引起系统崩溃。拒绝服务攻击对通信系统的破坏作用尤为严重，因为通信系统是专门用于通信的，对网络上一台计算机提出大量的通信请求，最易使该台计算机崩溃，且难以跟踪攻击源。

（2）邮件炸弹

邮件炸弹是另一种非常有效的拒绝服务攻击。给某人发送过量的电子邮件可使他的系统满载直至崩溃，这种攻击最简单的办法就是向受害者发送成千上万的电子邮件，这样做会耗尽受害者的硬盘空间，使网络连接被迫中断，或者使计算机系统崩溃，且难以找到攻击者。

拒绝服务攻击的对象不同，可以是邮件服务器、路由器或 Web 服务器等。其基本思路大致相同，即向目标发送大量信息使其崩溃。有效的应对方式是在 ISP 端进行大规模的过滤，如果网络能阻止拒绝服务攻击，那么这种攻击就不会伤及目标计算机。但 ISP 过滤不仅需做大量的工作，而且会使网络带宽明显下降。有些攻击还利用了系统的某些脆弱性进行大流量攻击。有人提议将让客户端在连接网络时进行稍复杂的计算作为一种防范措施。如果客户机需花费一定时间才能完成一个网络连接，那么它就不能与目标机进行大量的连接。但这对于分布式拒绝服务攻击却无效。

4. 分布式拒绝服务（DDoS）攻击

分布式拒绝服务攻击是拒绝服务群起进攻的方式。这种攻击与传统的拒绝服务攻击一样，只不过进攻源不止一个。黑客首先进入成百上千没有安全防护系统的计算机，入侵

者在计算机内安装一个攻击程序,之后他控制这些计算机同时向目标发起进攻。目标机即刻受到来自多个地方的攻击,传统的防范措施失去作用,最终发生死机。

在传统方式的拒绝服务攻击中,作为受害者的计算机可能会察觉攻击源,并关闭这些连接。但在分布式拒绝服务攻击中,进攻源不止一个,计算机应关闭除它信任的连接之外的所有连接,但这在公共 Internet 站点上根本无法实现。迄今为止,对分布式拒绝服务攻击还没有通用的防护手段。只有不断监视网络连接,及时切换备份服务器和路由器。有时一些特殊的被攻击行为利用的漏洞可以修复,但很多却不能。

上面列举的一些网络安全问题,充分说明与计算机信息系统安全相比,在分布网络环境下,出现了很多新的安全问题,而且有些老的安全问题也以不同的形式出现。根据这些特点,给出以下的网络安全定义:

网络安全是在分布网络环境中,对信息载体(处理载体、存储载体、传输载体)和信息的处理、传输、存储、访问提供安全保护,以防止数据、信息内容或能力被非授权使用、篡改或拒绝服务。

维护信息载体的安全就要抵抗对网络和系统的安全威胁。这些安全威胁包括物理侵犯(如机房侵入、设备偷窃、废物搜寻、电子干扰等)、系统漏洞(如旁路控制、程序缺陷等)、网络入侵(如窃听、截获、堵塞等)、恶意软件(如病毒、蠕虫、特洛伊木马、信息炸弹等)、存储损坏(如老化、破损等)等。为抵抗对网络和系统的安全威胁,通常采取的安全措施包括门控系统、防火墙、防病毒、入侵检测、漏洞扫描、存储备份、日志审计、应急响应、灾难恢复等。

维护信息自身的安全就要抵抗对信息的安全威胁。这些安全威胁包括身份假冒、非法访问、信息泄露、数据受损、事后否认等。为抵抗对信息的安全威胁,通常采取的安全措施包括身份鉴别、访问控制、数据加密、数据验证、数字签名、内容过滤、日志审计、应急响应、灾难恢复等。

1.1.2　网络安全的属性

网络安全具有三个基本属性。

1. 机密性(保密性)

机密性是指保证信息与信息系统不被非授权者所获取与使用,主要防范措施是密码技术。

在网络系统的各个层次上有不同的机密性及相应的防范措施。在物理层,要保证系统实体不以电磁的方式(电磁辐射、电磁泄露)向外泄露信息,主要的防范措施是电磁屏蔽技术、加密干扰技术等。在运行层面,要保障系统依据授权提供服务,使系统任何时候不被非授权人所使用,对黑客入侵、口令攻击、用户权限非法提升、资源非法使用等采取漏洞扫描、隔离、防火墙、访问控制、入侵检测、审计取证等防范措施,这类属性有时也称为可控性。在数据处理、传输层面,要保证数据在传输、存储过程中不被非法获取、解析,主要防范措施是数据加密技术。

2 完整性

完整性是指信息是真实可信的,其发布者不被冒充,来源不被伪造,内容不被篡改,主

要防范措施是校验与认证技术。

在运行层面，要保证数据在传输、存储等过程中不被非法修改，防范措施是对数据的截获、篡改与再送采取完整性标识的生成与检验技术。要保证数据的发送源头不被伪造，对冒充信息发布者的身份、虚假信息发布来源采取身份认证技术、路由认证技术，这类属性也可称为真实性。

3. 可用性

可用性是指保证信息与信息系统可被授权人正常使用，主要防范措施是确保信息与信息系统处于一个可靠的运行状态之下。

在物理层，要保证信息系统在恶劣的工作环境下能正常运行，主要防范措施是对电磁炸弹、信号插入采取抗干扰技术、加固技术等。在运行层面，要保证系统时刻能为授权人提供服务，对网络被阻塞、系统资源超负荷消耗、病毒、黑客等导致系统崩溃或宕机等情况采取过载保护、防范拒绝服务攻击、生存技术等防范措施。保证系统的可用性，使得发布者无法否认所发布的信息内容，接收者无法否认所接收的信息内容，对数据抵赖采取数字签名防范措施，这类属性也称为抗否认性。

从上面的分析可以看出，维护信息载体的安全与维护信息自身的安全两个方面都含有机密性、完整性、可用性这些重要属性。

1.1.3　网络安全层次结构

国际标准化组织在开放系统互连标准中定义了 7 个层次的网络参考模型，它们分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。不同的网络层次之间的功能虽然有一定的交叉，但是基本上是不同的。例如，数据链路层负责建立点到点通信，网络层负责寻径，传输层负责建立端到端的通信信道。从安全角度来看，各层能提供一定的安全手段，针对不同层的安全措施是不同的。

要对网络安全服务所属的协议层次进行分析，一个单独的层次无法提供全部的网络安全服务，每个层次都能做出自己的贡献。

在物理层，可以在通信线路上采用某些技术使得搭线偷听变得不可能或者容易被检测出。

在数据链路层，点对点的链路可能采用通信保密机进行加密和解密，当信息离开一台机器时进行加密，而进入另外一台机器时进行解密。所有的细节可以全部由底层硬件实现，高层根本无法察觉。但是这种方案无法适应需要经过多个路由器的通信信道，因为在每个路由器上都需要进行加密和解密，在这些路由器上会出现潜在的安全隐患，在开放网络环境中并不能确定每个路由器都是安全的。当然，链路加密无论在什么时候都是很容易而且有效的，也被经常使用，但是在 Internet 环境中并不完全适用。

在网络层，使用防火墙技术处理信息在内外网络边界的流动，确定来自哪些地址的信息可能或者禁止访问哪些目的地址的主机。

在传输层，这个连接可能被端到端的加密，也就是进程到进程间的加密。虽然这些解决方案都有一定的作用，并且有很多人正在试图提高这些技术，但是他们都不能提出一种

充分通用的办法来解决身份认证和不可否认问题。这些问题必须要在应用层解决。

应用层的安全主要是指针对用户身份进行认证并且建立起安全的通信信道。有很多针对具体应用的安全方案，它们能够有效地解决诸如电子邮件、HTTP 等特定应用的安全问题，能够提供包括身份认证、不可否认、数据保密、数据完整性检查乃至访问控制等功能。但是在应用层并没有一个统一的安全方案，通用安全服务 GSS-API 的出现试图将安全服务进行抽象，为上层应用提供通用接口。在 GSS-API 接口下可以采用各种不同的安全机制来实现这些服务。

总结前面的讨论，可以用图 1-1 来表示网络安全层次。

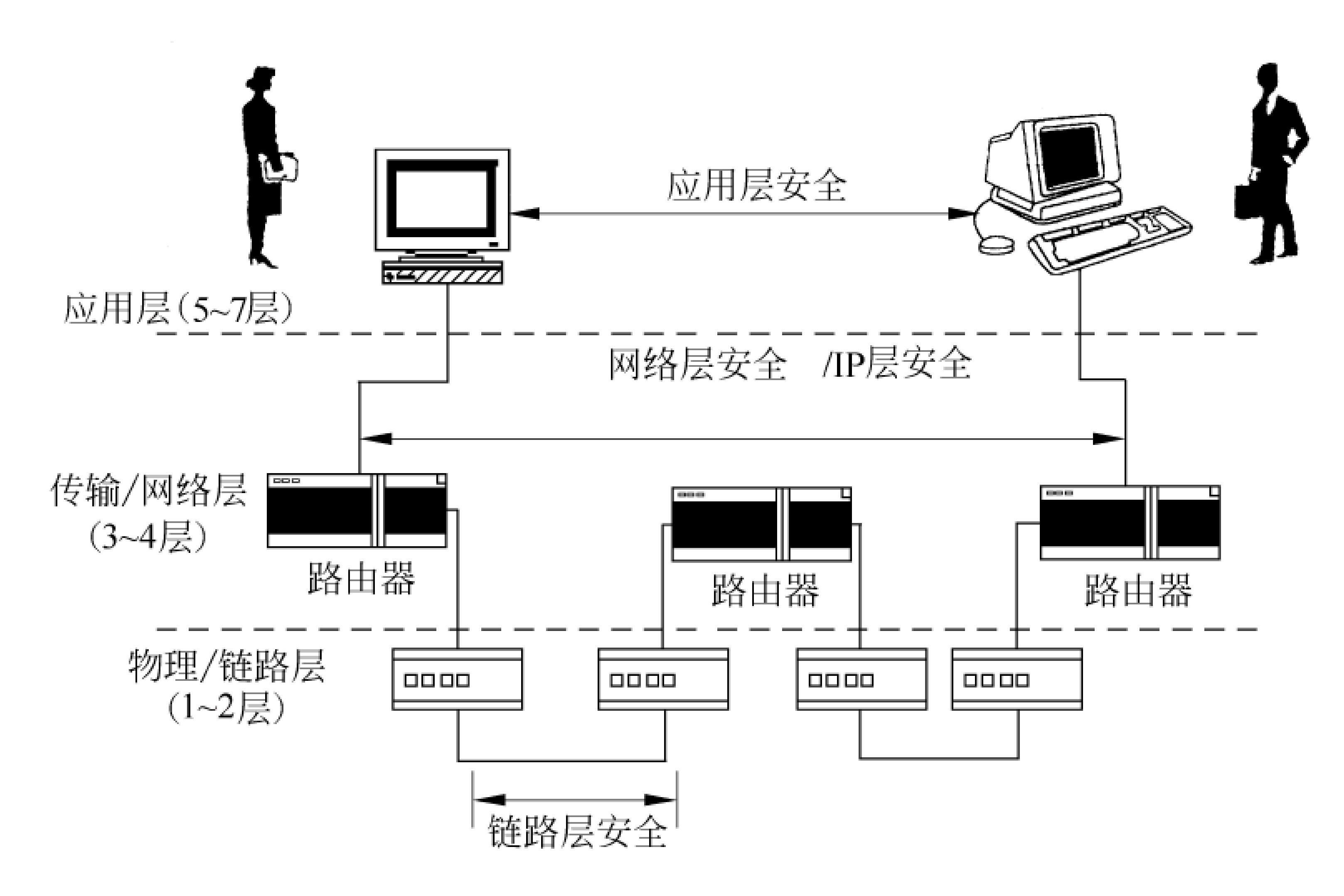


图 1-1　网络安全层次图

1.1.4　网络安全模型

图 1-2 给出了网络安全模型，报文从源站经网络（Internet）送至目的站，源站和目的站是处理的两个主体，它们必须协同处理这个交换。建立逻辑信息通道的目的是确定从源站经 Internet 到目的站的路由以及两个主体协同使用诸如 TCP/IP 的通道协议。

为了在开放网络环境中保护信息的传输，需要提供安全机制和安全服务，主要包含两个部分：一部分是对发送的信息进行与安全相关的转换。例如，报文的加密，使开放网络对加密的报文不可读；又如，附加一些基于报文内容的码，用来验证发送者的身份。另一部分是由两个主体共享的秘密信息，而对开放网络是保密的。例如，用以加密转换的密钥，用于发送前的加密和接收前的解密。

为了完成安全的处理，常常需要可信的第三方。例如，第三方可负责为两个主体分发秘密信息，而对开放网络是保密的；又如，需要第三方来仲裁两个主体在报文传输的身份认证的争执。

归纳起来，在设计网络安全系统时，该网络安全模型应完成 4 个基本任务：

（1）设计一个算法以实现和安全有关的转换。

（2）产生一个秘密信息用于设计的算法。

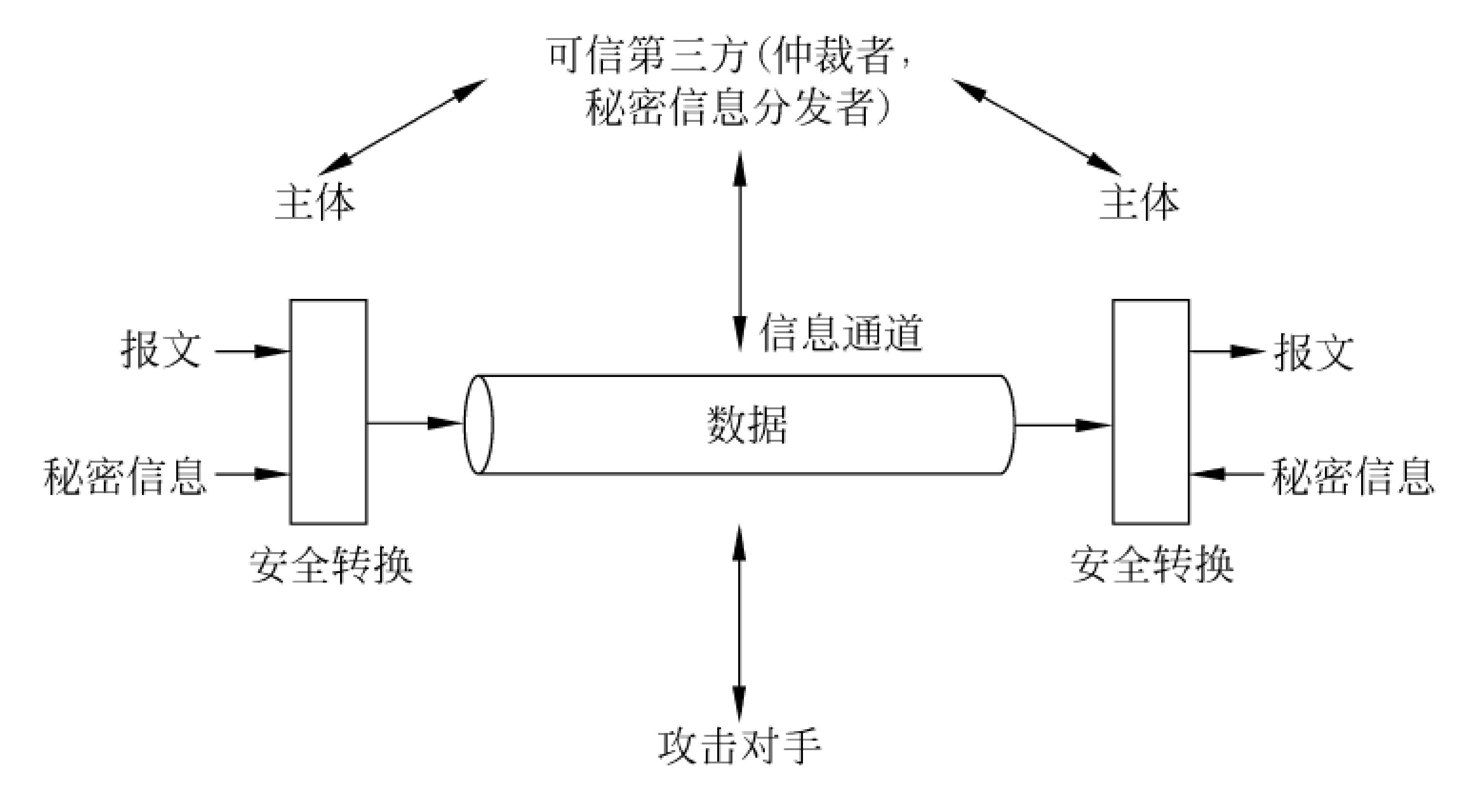


图 1-2　网络安全模型

(3) 开发一个分发和共享秘密信息的方法。

(4) 确定两个主体使用的协议,用于使用秘密算法与秘密信息以得到特定的安全服务。

图 1-2 的网络安全模型虽是一个通用的模型,但它并不能涵盖所有情况。图 1-3 给出了一个网络访问安全模型,该模型考虑了黑客攻击、病毒与蠕虫等的非授权访问。黑客攻击可以形成两类威胁:一类是信息访问威胁,即非授权用户截获或修改数据;另一类是服务威胁,即服务流激增以禁止合法用户使用。病毒和蠕虫是软件攻击的两个实例,这类攻击通常是通过移动存储介质引入系统,并隐藏在有用软件中;也可通过网络接入系统。

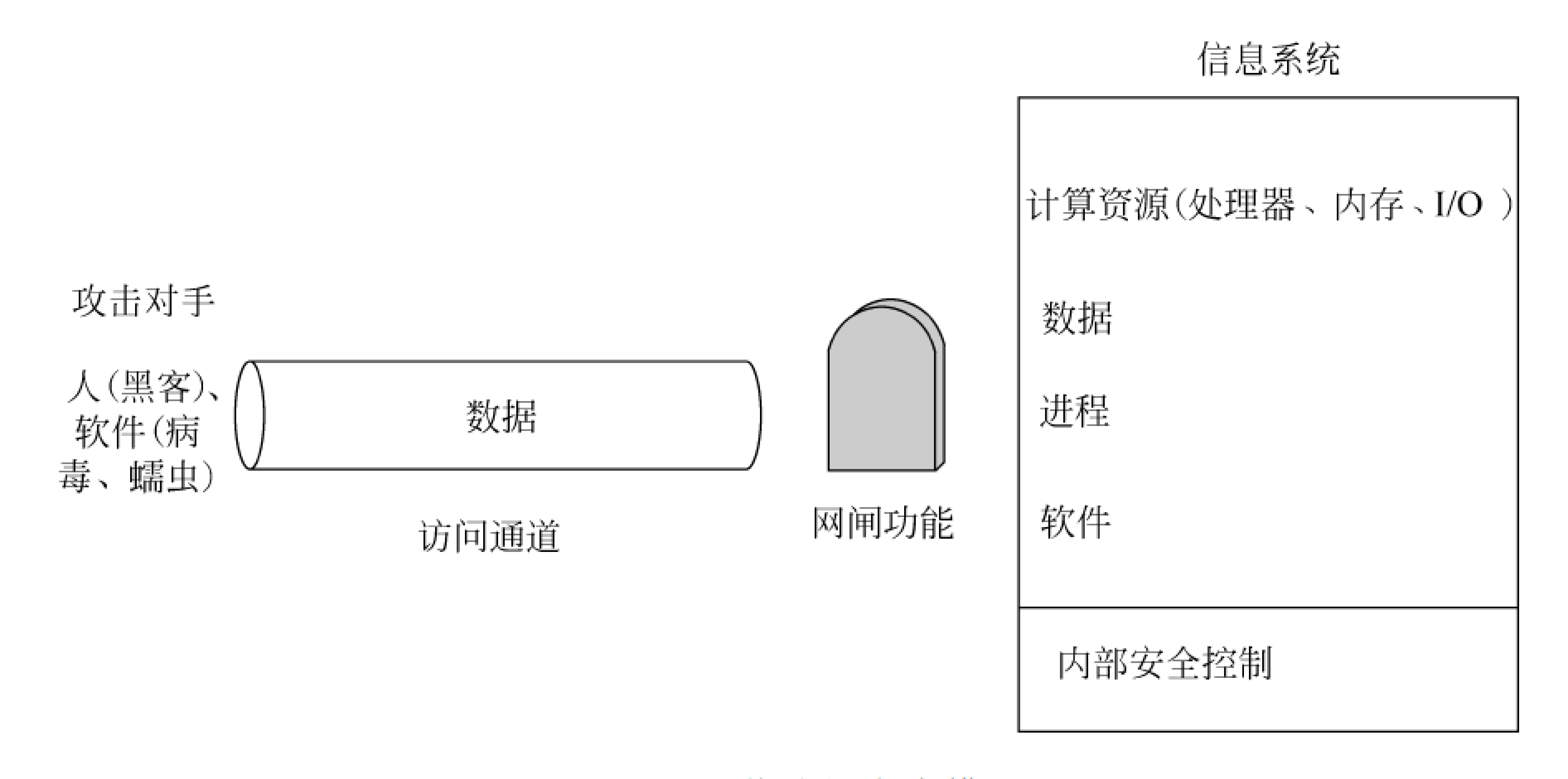


图 1-3　网络访问安全模型

在图 1-3 中,对非授权访问的安全机制可分为两类:第一类是网闸功能,包括基于口令的登录过程以拒绝所有非授权访问以及屏蔽逻辑以检测、拒绝病毒、蠕虫和其他类似攻击;第二类是内部的安全控制,一旦非授权用户或软件攻击得到访问权,第二道防线将对其进行防御,包括各种内部控制的监控和分析,以检测入侵者。

1.2 安全的历史回顾

随着社会和技术的进步，信息安全也有一个发展的过程，了解信息安全的发展历史，可使人们更全面地解决当前遇到的各种信息安全问题。粗略地，可把信息安全分成 3 个阶段，即通信安全(comsec)、计算机安全(compusec)和网络安全(netsec)。

1.21 通信安全

早期，所有的资产都是物理的，重要的信息也是物理的，如古代刻在石头上，到后来写在纸上。为了保护这些资产，只需要用墙、护城河、警卫等物理安全措施。信息传递通常由信使完成，需要时可带有警卫。除非用物理的掠夺，否则就无法得到信息。

但是，物理安全存在缺陷，如果报文在传递中被截获，则报文的信息就会被敌人知悉。因此就产生了通信安全的问题。早在公元前 600 年 Julius Caesar 生成了 Caesar 密码，以使报文即使被截获也无法读出。

这个概念一直延续到第二次世界大战，德国人使用一种称为 Enigma 的机器来加密报文，用于军队，当时他们认为 Enigma 是不可破译的。确实是这样，如果使用恰当，要破译它非常困难。但经过一段时间发现，由于某些操作员的使用差错，Enigma 被破译了。

军事通信也使用编码技术，将每个字编码后放入报文传输。在战争期间，日本人曾用编码后的字通信，即使美国人截获了这些编码也难以识别该报文。在准备 Midway 之战时，日本人曾传送编码后的报文，使日美之间在编码和破译方面展开了一场有关通信安全的对抗。

为了防止敌人窃听语音报文，美国军队曾使用一种 Navaho 码的步话机，Navaho 用本土语言传送报文，敌人即使收听到无线电通信，也无法懂得报文的意思。

第二次世界大战后，苏联间谍曾经使用一次填充来保护传递的信息。一次填充的方法是在每一页上用带有随机数的文字填充，每一页只用一个报文。这个加密方案如果使用正确则难以破译。但是由于他们的使用方法不正确(重用一次填充)，结果某些报文被破译出来。

从上面这些事例可知，通信安全的主要目的是解决数据传输的安全问题，主要的措施是密码技术。

除非不正确地使用密码系统，一般来说，好的密码难以破译。因此人们企图寻找别的方法来截获加密传输的信息。在 20 世纪 50 年代发现了寻找在电话线上的信号来达到获取报文的目的。如图 1-4 所示。所有的电子系统都会释放电子辐射，包括电传机和正在使用发送加密报文的密码机。密码机将报文加密，并且通过电话线发送出去。可是发现代表原始信号的电信号也能在电话线上发现，这意味着可用某种好的设备来恢复原始信号。这个问题导致美国开发一个称为 TEMPEST 的计划，它制定了用于十分敏感环境的计算机系统电子辐射标准。其目的是降低辐射以免信号被截获。

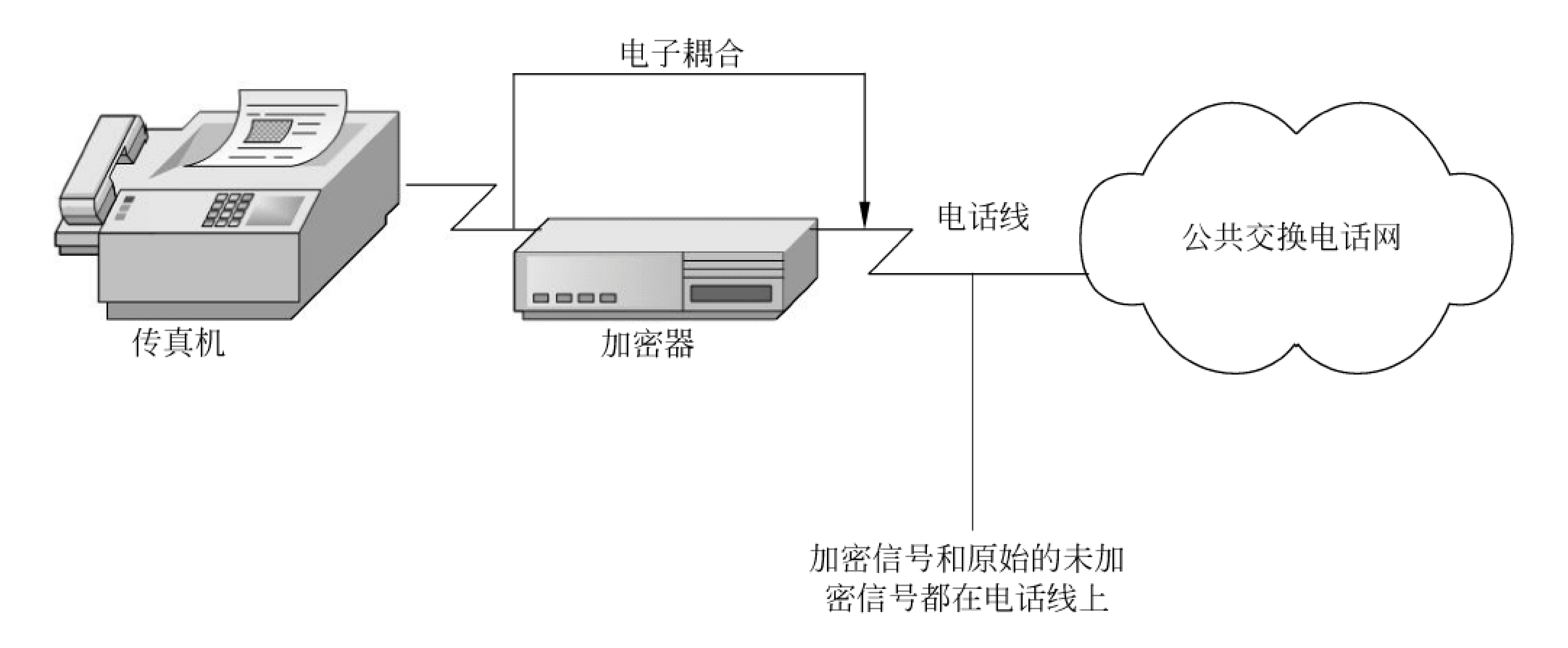


图 1-4　旁路密码的电子信号

1.22　计算机安全

随着计算机技术及其应用的发展，各个单位的大部分信息资产以电子形式移植到计算机上。计算机的使用越来越方便，更多的人用交互会话的方式访问信息。计算机系统上的信息对任何访问系统的人都是可访问的。

在 20 世纪 70 年代，David Bell 和 Leonard La Padula 开发了一个安全计算机的操作模型。该模型是基于政府概念的各种级别分类信息（一般、秘密、机密、绝密）和各种许可级别。如果主体的许可级别高于文件（客体）的分类级别，则主体能访问客体。如果主体的许可级别低于文件（客体）的分类级别，则主体不能访问客体。

这个模型的概念进一步发展，于 1983 年导出了美国国防部标准 5200.28——可信计算机系统评估准则（Trusted Computer System Evaluation Criteria，TCSEC），即橘皮书。TCSEC 共分为如下 4 类 7 级：

（1）D 级，安全保护欠缺级。

（2）C1 级，自主安全保护级。

（3）C2 级，受控存取保护级。

（4）B1 级，标记安全保护级。

（5）B2 级，结构化保护级。

（6）B3 级，安全域保护级。

（7）A1 级，验证设计级。

橘皮书对每一级都定义了功能要求和保证要求，也就是说要符合某一安全级要求，必须既满足功能要求，又满足保证要求。为了使计算机系统达到相应的安全要求，计算机厂商要花费很长时间和很多资金。有时当某产品通过级别论证时，该产品已经过时了。计算机技术发展得如此之迅速，当老的系统取得安全认证之前新版的操作系统和硬件已经出现。

欧洲四国（荷兰、法国、英国、德国）在吸收了 TCSEC 的成功经验基础上，于 1989 年联合提出了信息技术安全评估准则（Information Technology Security Evaluation

Criteria，ITSEC)，俗称白皮书，其中首次提出了信息安全的机密性、完整性、可用性的概念，把可信计算机的概念提高到可信信息技术的高度。

之后，由美国国家标准技术研究所(NIST)、国家安全局(NSA)、欧洲四国以及加拿大6国7方联合提出了通用安全评估准则(Command Criteria for IT Security Evaluation，CC)，并于1991年宣布，1995年发布正式文件。它的基础是欧洲的白皮书ITSEC、美国的(包括橘皮书TCSEC在内的)新的联邦评估准则、加拿大的CTCPEC以及国际标准化组织的ISO/SCITWGS的安全评估标准。

我国国家质量技术监督局也于1999年发布了计算机信息系统安全保护等级划分准则(Classified Criteria for Security Protection of Computer Information System)的国家标准，序号为GB 17859－1999，评估准则的制定为我们评估、开发、研究计算机系统的安全提供了指导准则。

计算机安全的主要目的是解决计算机信息载体及其运行的安全问题，主要措施是根据主、客体的安全级别，正确实施主体对客体的访问控制。

1.2.3　网络安全

当计算机联成网络以后，新的安全问题出现了，老的安全问题也以不同的形式出现。例如，各种局域网、城域网的安全不同于以往的远距离点到点的通信安全；又如，高速网络以及由很多连接器连到一个公共的通信介质，原有的专用密码机已经完全不能解决问题；再如，有很多用户从不同的系统经过网络访问，而没有单个计算机的集中控制。

随着Internet的发展及其普及应用，如何解决在开放网络环境下的安全问题更成为迫切需要解决的问题。如上面所述的IP安全、DNS安全、拒绝服务与分布拒绝服务攻击等。

橘皮书并不解决联网计算机的问题，事实上，网络的访问在橘皮书的认证中是无效的。为此，美国国防部于1987年制定了TCSEC的可信网络解释TNI，又称红皮书。除了满足橘皮书的要求外，红皮书还企图解决计算机的联网环境的安全问题。红皮书主要说明联网环境的安全功能要求，较少阐明保证要求。

网络安全的主要目的是解决在分布网络环境中对信息载体及其运行提供的安全保护问题，主要措施是提供完整的信息安全保障体系，包括防护、检测、响应、恢复。

1.3　网络安全挑战

网络安全，尤其是Internet安全正面临着严重的挑战，主要是：

- Internet规模的扩大和关键应用的激增；
- 网络安全攻击的持续增加、安全漏洞的增长；
- 网络安全的对策(技术、人才、立法)急需开发。

1.3.1　Internet规模及应用激增

Internet是一个全球的计算机互联网，在发展初期规模不大，主要应用于高等学校和

科研机构,并假定它的用户能互相认识和信任。然而,随着 Internet 的发展和流行,用户数量不断增长,网络应用日益普及,黑客攻击的激增,使得这种信任模式恶化。

20 世纪 90 年代开始,Internet 的应用扩展了新的领域,以电子商务为代表的应用,创建了一个开展业务的重要渠道,为了及时和安全地交付这些电子商务系统,对网络安全提出了更高的要求。还有像电子政务这类关键应用也都必须有安全保证。Internet 在初期完全开放的设计特性而没有考虑安全的情况已不适应当代的要求。

1999 年采用的 802.1 无线局域网协议使移动计算产业发生了革命,但同时也增加了不安全的风险。一方面运行环境的保护必须延伸到接到无线网上的计算机;另一方面 802.11 协议的安全特性很弱。

表 1-1 列出了互联网和无线互联网用户数量与分布。

表 1-1　互联网和无线互联网用户数量与分布

地区 \ 年份	2001	2004	2007
美国互联网用户(百万)	149	193	236
美国无线互联网用户所占比例	4.5%	27.9%	46.3%
全球互联网用户(百万)	533	945	1460
全球无线互联网用户所占比例	16.0%	41.5%	56.8%
亚太互联网用户(百万)	115	357	612
亚太无线互联网用户所占比例	34.8%	50.9%	60.4%
西欧互联网用户(百万)	126	208	290
西欧无线互联网用户所占比例	13.9%	49.6%	67.0%

1.3.2　网络安全攻击持续增加

自 1988 年莫里斯蠕虫发作,使 Internet 上 10%的计算机宕机,之后重大网络安全事件不断发生,这些攻击每年导致上百亿美元的损失。表 1-2 列出了历年重大网络安全事件。图 1-5 列出了更多的网络安全事件,包括重大的和影响相对较弱的。

表 1-2　重大网络安全事件

名称	日期	影响
莫里斯(Morris)蠕虫	1988 年	使与因特网连接的 10%的计算机宕机
梅丽莎(Melissa)	1999 年 5 月	在一周内感染 100 000 台计算机,15 亿美元经济影响
Explorer 病毒	1999 年 6 月	11 亿美元经济影响
爱虫(I Love You)病毒	2000 年 5 月	87.5 亿美元经济影响
Cam 先生(Sircam)病毒	2001 年 7 月	230 万台计算机被感染,12.5 亿美元经济影响

续表

名　　称	日　期	影　　响
红色代码(Code Red)蠕虫	2001 年 7 月	在不到 14 个小时内,359 000 台计算机被感染
尼姆达(Nimda)蠕虫	2001 年 9 月	高峰时 160 000 台计算机被感染 15 亿美元经济影响
求职信(Klez)	2002 年	7.5 亿美元经济影响
顽皮熊(BugBear)	2002 年	5 亿美元经济影响
Badtrands	2002 年	4 亿美元经济影响
蓝宝石/蠕虫王(Sapphire/Slammer)蠕虫	2003 年 1 月	仅仅 10 分钟内,就感染了 90%的具有相应弱点的主机,高峰时有 75 000 台计算机被感染,15 亿美元经济影响
冲击波(Blaster)	2003 年	7.5 亿美元经济影响
冲击波杀手(Nachi)	2003 年	5 亿美元经济影响
大无级(SoBig. F)	2003 年	25 亿美元经济影响
悲惨命运(MyDoom)蠕虫	2004 年 1 月	到目前为止传播最快的邮件蠕虫,每小时有 100 000 个蠕虫被拦截,超过 40 亿美元的经济影响
机智(Witty)蠕虫	2004 年 3 月	第一个携带破坏性网络数据内容并广泛传播的蠕虫
震荡波(Sasser)	2004 年 5 月	破坏超过冲击波
Zobot 蠕虫	2005 年 8 月	

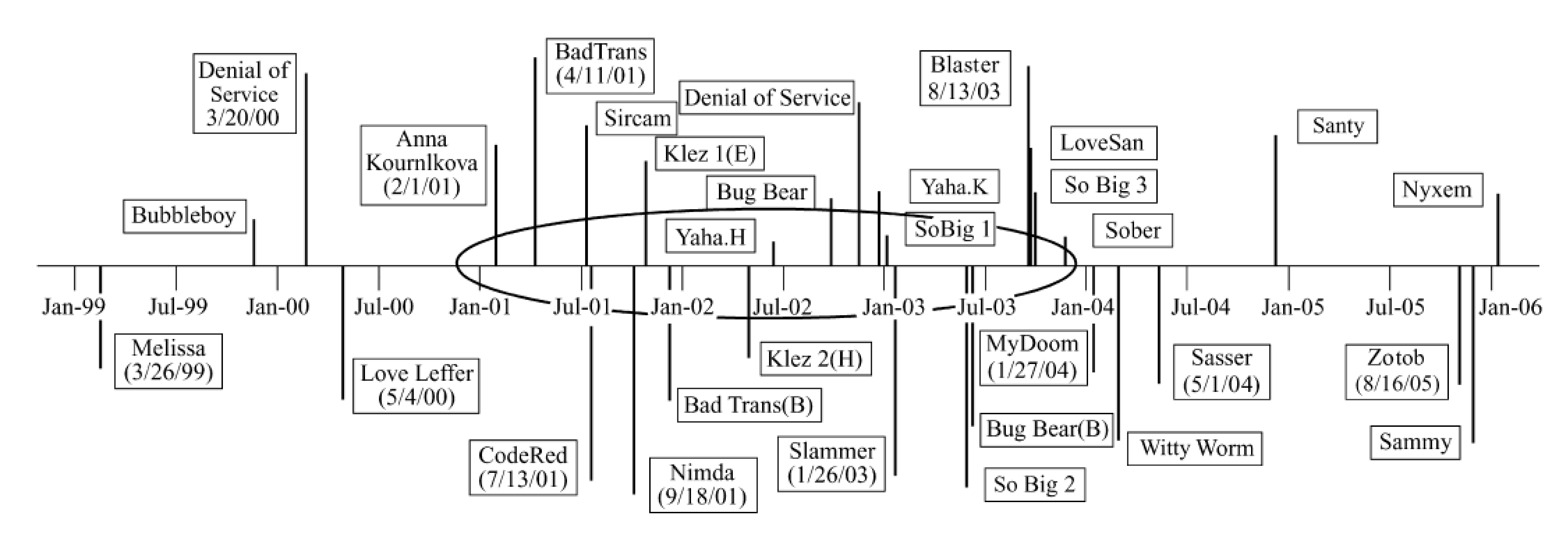


图 1-5　网络安全事件

据统计,Internet 每天受到的攻击数达 4 967 541 次,平均每小时 206 981 次攻击或每分钟 3450 次攻击。图 1-6 显示恶意代码攻击在世界范围造成的损失。

有三个重要的因素加剧了安全事件数量的增加:不断增加的系统漏洞数量、在应付系统漏洞的过程中需要大量人工及攻击本身的复杂性。

漏洞是指一个系统中可以被黑客用来攻击或危害系统的突破口或弱点。针对这些系统漏洞,软件行业的解决方案是以软件补丁的形式提供修复方式,用户必须使用它来修补这些后门。在 IT 环境中测试并应用这些补丁的过程需要繁重的劳动,通常寻找并修补最高级别的漏洞是十分困难的,而且还会不断涌现新的漏洞。图 1-7 显示安全漏洞数历

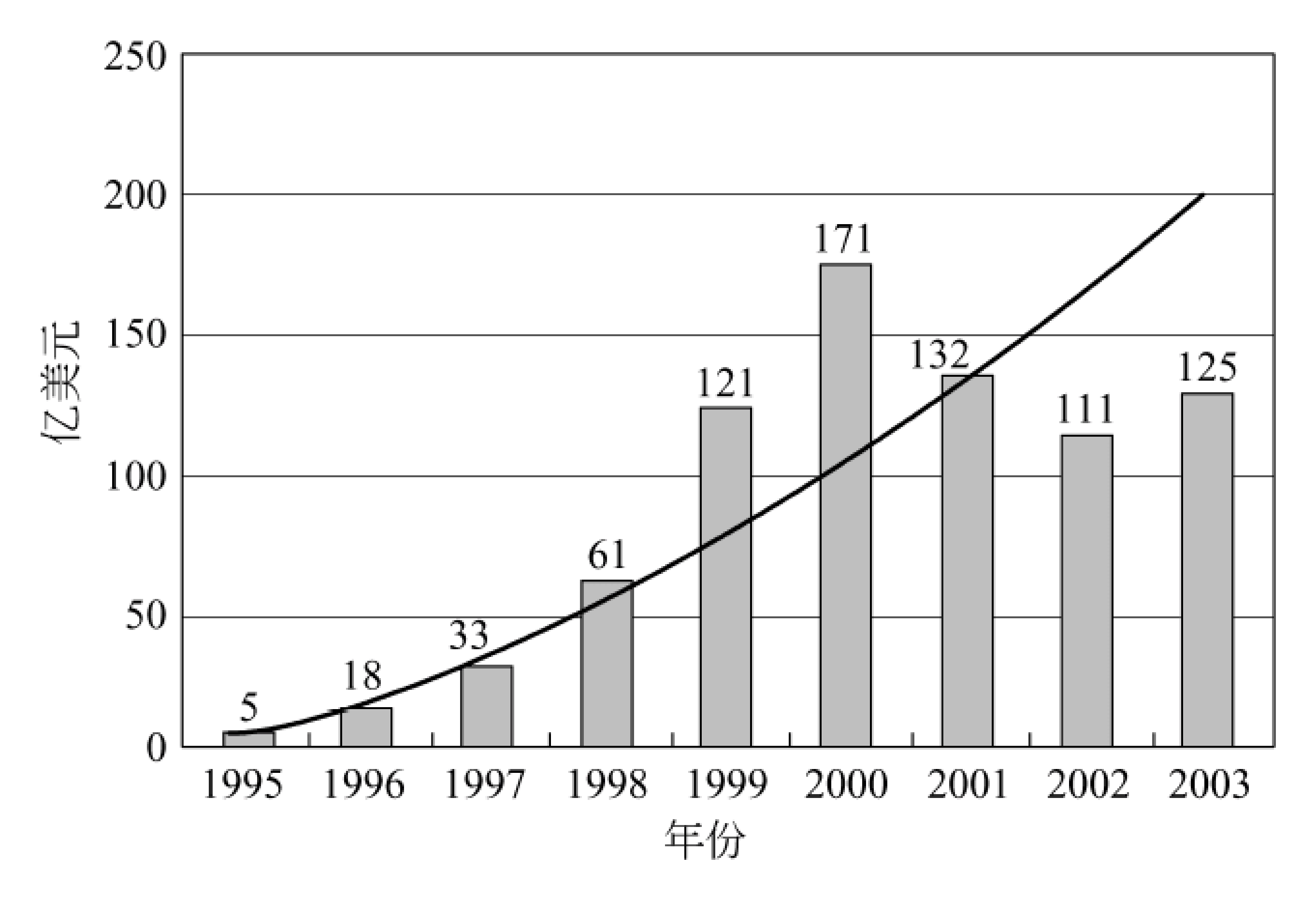


图 1-6　恶意代码在世界范围造成的损失

年增长的情况。

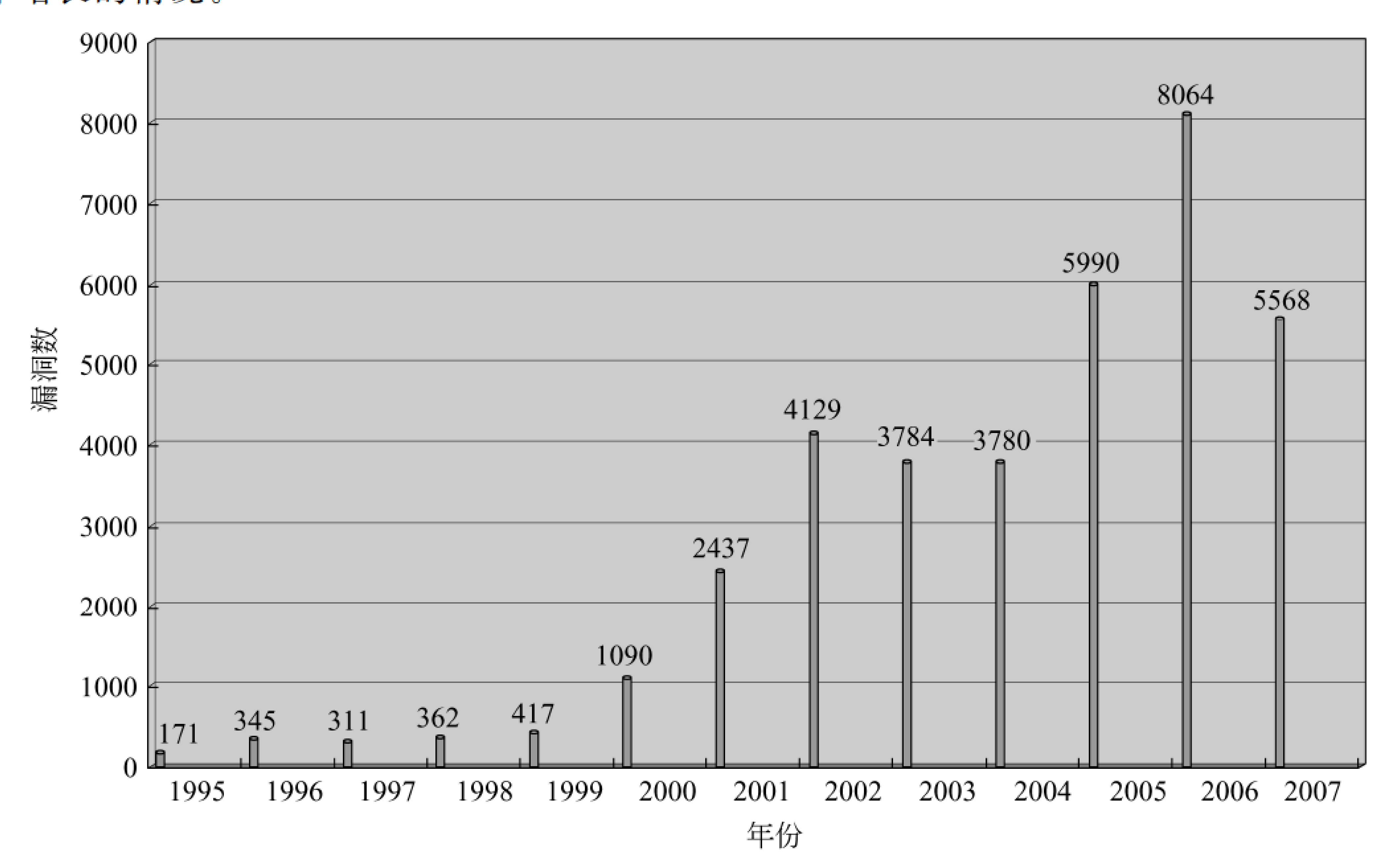


图 1-7　安全漏洞数的增长

在过去几年中，安全攻击的复杂性增加了很多。早期的病毒只会使个人生产力下降，它们的影响远不及诸如红色代码和尼姆达这样的混合威胁。混合威胁使用组合的攻击方式来更快地传播，并且造成比单个病毒更大的危害。以红色代码为例，它曾在 14 小时内感染了 350 000 多台计算机。在 2003 年 1 月蠕虫王袭击了 Internet，它具有比红色代码更高的传染率，在被释放后不到 10 分钟内，就感染了 75 000 台计算机。

到目前为止，传播最快的群发邮件蠕虫是 2004 年 1 月爆发的“悲惨命运”。在爆发的高峰期，每小时截获的蠕虫样本数超过 100 000 个。“悲惨命运”依靠用户去激活并开始传播。它聪明地伪装成一个没有恶意的文本附件，毫无戒备心的用户打开附件时就启动了蠕虫。

这些迅速传播的威胁使得人为的快速响应并阻止危害变得愈加困难。从世界范围内攻击的发展趋势来看，网络入侵活动愈益增加，并超过了恶意代码感染活动的次数，图 1-8 显示了这种发展趋势。另一个发展趋势是入侵攻击变得愈加容易，攻击技巧不断提高，要求攻击者的知识反而降低了。图 1-9 显示了这种发展趋势。

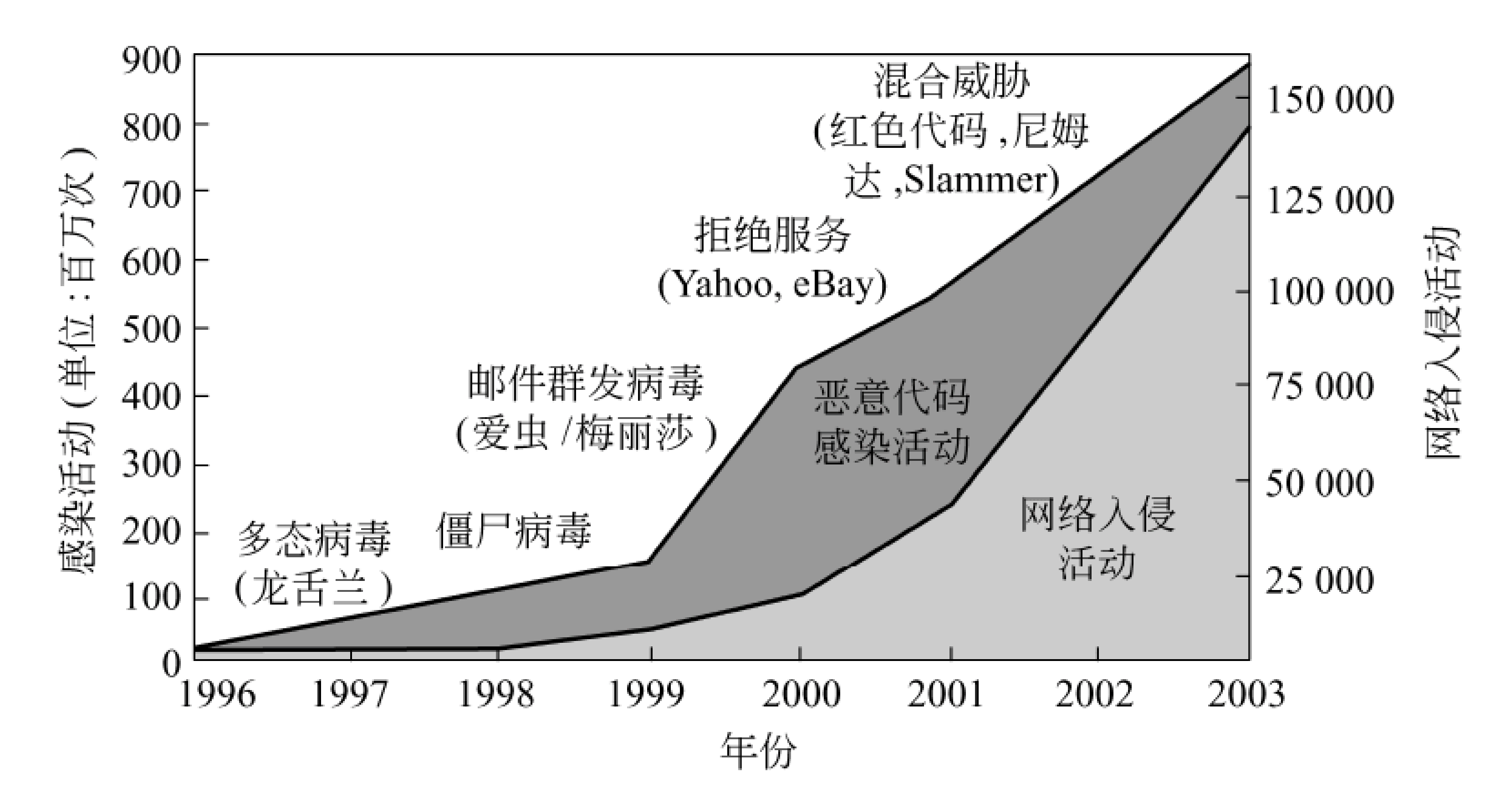


图 1-8　世界范围内攻击的发展趋势

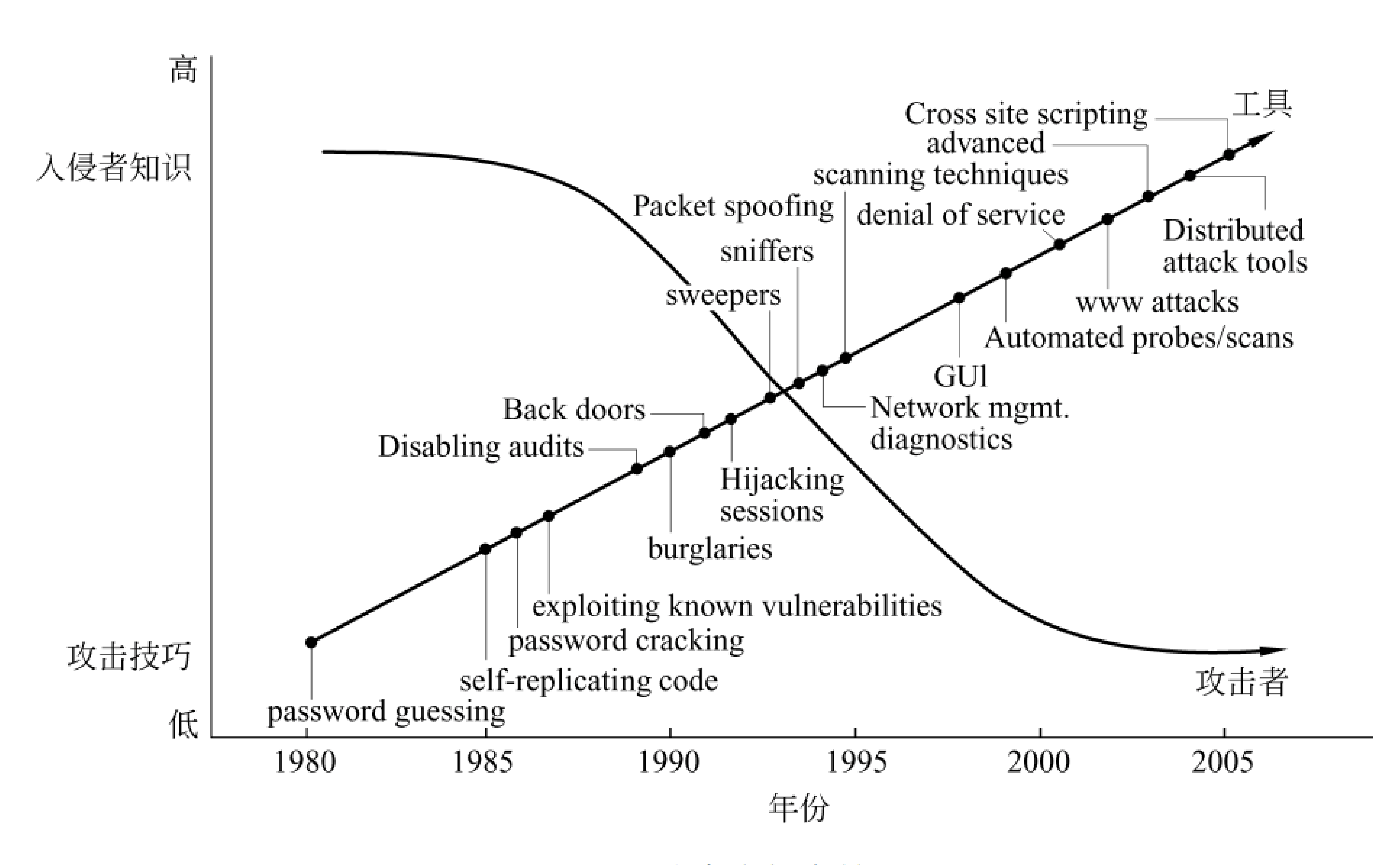


图 1-9　攻击愈加容易

面对这严峻的形势，网络安全对策(技术、人才、立法)急需开发。然而当前信息安全市场尚不成熟，信息安全厂商还不能提供成熟的安全解决方案。信息安全人才缺乏，在人才方面最大的挑战可能就是如何寻找一个在安全领域具有广泛背景并能组建一支有效的信息安全团队的领军人物。信息安全事件激增及其严重危害，以及对 Internet 越来越多的依赖，促使世界各国政府开始制定特别的法律来管理和规范这个技术环境。因为 Internet 是全球化运营，必须遵守许多不同国家的法律法规，理解这些可能要面对的法律和限制是很重要的。

1.3.3 国内互联网发展及互联网安全状况

自 1994 年我国正式接入 Internet 以来，互联网的规模和应用迅速发展。2007 年 7 月中国互联网信息中心(CNNIC)发布的第 20 次中国互联网发展状况统计报告显示，我国网民总人数已达到 1.62 亿，普及率为 12.3%，上网计算机数达 6710 万。截至 2008 年 6 月底，我国网民数达到了 2.53 亿，首次大幅度超过美国，跃居世界第一位。然而，目前中国互联网安全状况不容乐观，各种网络安全事件与去年同期相比有明显增加。2007 年上半年国家计算机网络应急技术处理协调中心 CNCERT/CC 接收的网络仿冒事件和网页恶意代码事件，已分别超出上一年全年总数的 14.6% 和 12.5%，被植入木马的主机 IP 比上一年全年增加 21 倍，被篡改网站数量比去年同期增加 4 倍。

攻击者攻击目标明确，针对不同网站和用户用不同的攻击手段。对政府类和安全管理相关的网站主要采用篡改网页的攻击形式；对以网络为核心业务的企业，采用有组织的分布式拒绝服务(DDoS)攻击等手段进行勒索；对个人用户是通过用户身份窃取等手段偷取账号、密码，窃取用户私人财产；对金融机构网上交易用网络钓鱼进行网络仿冒，在线盗用用户身份和密码。通过恶意网页、电子邮件和信息系统漏洞等方式传播恶意代码，利用间谍软件和木马程序窃取用户的私有信息，严重导致财产损失。2007 年上半年我国内地被植入木马的主机数量大幅攀升。

2007 年上半年恶意代码的目的性增强。僵尸网络发展迅速，逐渐成为攻击行为的基本渠道。针对 DNS 服务器和域名转发服务器的攻击数量有明显增多的趋势。新型网络应用的发展带来了新的安全问题和威胁。

近半年，各种网络安全事件数量有显著增加，说明我国公共互联网面临着更加严重的安全威胁，而以获利为目的的攻击事件将对广大用户造成更加直接的经济损失。

1.4 密码学

1.4.1 密码学的基本原理

密码学是以研究数据保密为目的，对存储或者传输的信息采取秘密的交换以防止第三者对信息的窃取的技术。被变换的信息称为明文(plaintext)，它可以是一段有意义的文字或者数据；变换过后的形式称为密文(ciphertext)，密文应该是一串杂乱排列的数据，从字面上没有任何含义。从明文到密文的变换过程称为加密(encryption)，变换本身是一个以加密密钥 k 为参数的函数，记作 $E_k(P)$。密文经过通信信道的传输到达目的地后需要还原成有意义的明文才能被通信接收方理解，将密文 C 还原为明文 P 的变换过程称为解密或者脱密(decryption)，该变换是以解密密钥 k' 为参数的函数，记作 $D_{k'}(C)$。密码学加密解密模型如图 1-10 所示。

在传统密码体制中加密和解密采用的是同一密钥，即 $k=k'$，并且 $D_{k'}(E_k(P))=P$，称为对称密钥密码系统(Symmetric Key Cryptography)。现代密码体制中加密和解密采用不同的密钥，称为非对称密钥密码系统(Asymmetric Key Cryptography)，每个通信方

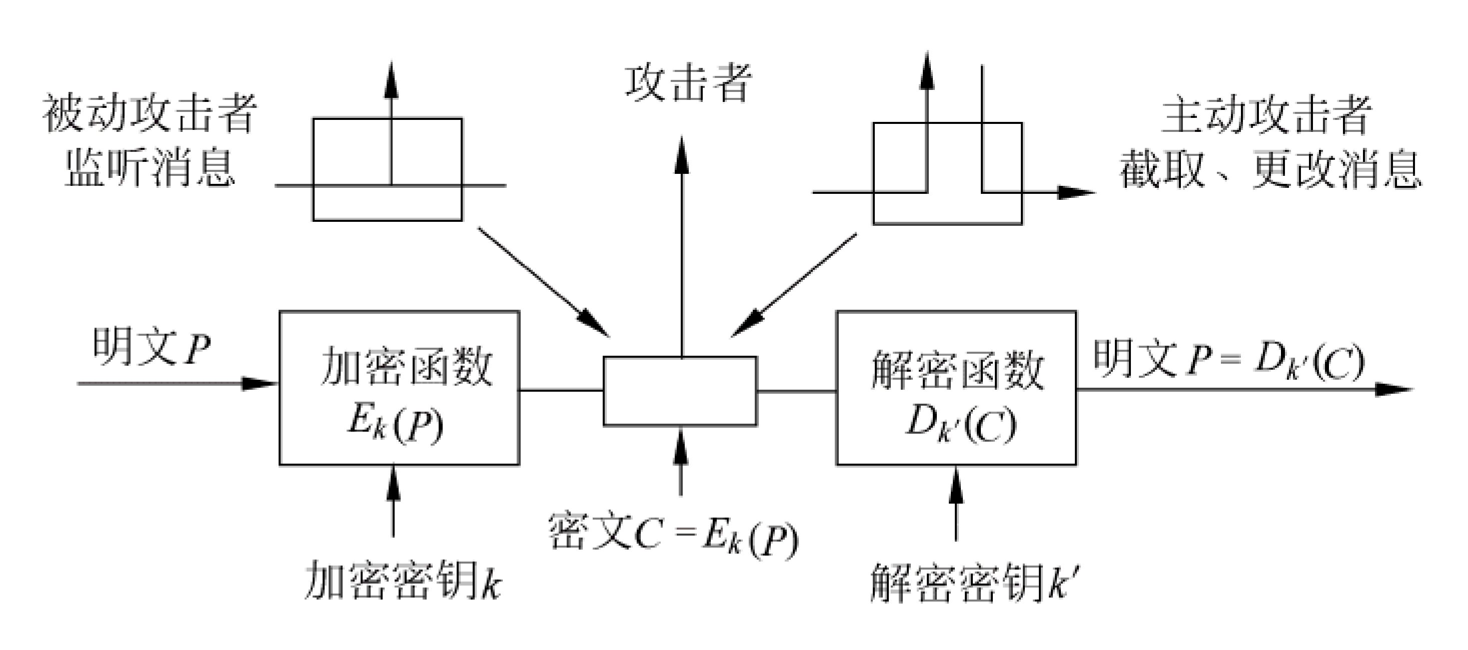


图 1-10　密码学模型

均需要有 k、k' 两个密钥，在进行保密通信时通常将加密密钥 k 公开（称为公钥 Public Key），而保留解密密钥 k'（称为私钥 Private Key），所以也称为公共密钥密码系统（Public Key Cryptography）。传统密码系统中最常见的算法有 DES、IDEA 等。DES（Data Encryption Standard，数据加密标准）算法是由 IBM 开发，并于 1997 年被美国政府采纳为非机密信息的加密标准，它的原始形式已经在 1995 年被攻破，但是修改后的形式仍然是有效的；IDEA（International Data Encryption Algorithm，国际数据加密算法）是由 Lai 和 Massey 提出的，目前还没有发现有效的攻击方法。

密码学研究包含两部分内容：一是加密算法的设计和研究；一是密码分析，即密码破译技术。在密码学模型中，假设进行密码分析的攻击者能够对密码通信进行攻击，能够被动地监听通信信道上的所有信息，称为被动攻击；他还能够对通信信道上传输的消息进行截取、修改甚至主动发送信息，称为主动攻击。攻击者与报文接收方的区别在于他不知道解密密钥，因此无法轻易将密文解密还原为明文。

公共密钥方案较对称密钥方案处理速度慢，因此，通常把公共密钥与对称密钥技术结合起来实现最佳性能，即用公共密钥技术在通信双方之间传送对称密钥，而用对称密钥来对实际传输的数据加密、解密。另外，公钥加密也用来对对称密钥进行加密。

在现代密码学研究中，对加密和解密算法一般都是公开的，对于攻击者来说，只要知道解密密钥就能够破译密文，因此，密钥设计成为核心，密钥保护也成为防止攻击的重点。对于密钥分析来说，对密钥进行穷举猜测攻击是任何密码系统都无法避免的，但是，当密钥长度足够随机时，应使穷举猜测实际上变得不可能。例如，密钥长度为 256 位的加密算法，密钥空间为 2^{256}，对应为 1077 量级，如果一台计算机每秒可以对密钥空间进行一亿次搜索，那么，全部搜索一遍的事件所需的时间将大于 1062 年。如果密钥空间小或者分布具有一定可预见性，那么，攻击者就可能利用相关知识缩小搜索空间，从而破译密文。

1.4.2　对称密钥密码技术

对称密钥密码技术是从传统的简单换位、代替密码发展而来的，自 1977 年美国颁布 DES 密码算法作为美国数据加密标准以来，对称密钥密码技术得到了迅猛发展，在世界各国得到广泛关注和使用。对称密钥密码技术从加密模式上可分为两类：

（1）序列密码

序列密码一直是作为军事和外交场合使用的主要密码技术之一，它的主要原理是，通

过有限状态机产生性能优良的伪随机序列，使用该序列加密信息流，逐位加密得到密文序列，所以，序列密码算法的安全强度完全取决于它所产生的伪随机序列的好坏。

(2) 分组密码

分组密码的工作方式是将明文分成固定长度的组(块)(如 64 位一组)，用同一密钥和算法对每一块加密，输出固定长度的密文。例如，DES 密码算法的输入为 64 位明文，密钥长度为 56 位，密文长度为 64 位。

设计分组密码算法的核心技术是，在相信复杂函数可以通过简单函数迭代若干圈得到的原则下，利用简单圈函数及对合等运算，充分利用非线性运算。以 DES 算法为例，它采用美国国家安全局精心设计的 8 个 S-Box 和 P-置换，经过 16 圈迭代，最终产生 64 位密文，每圈迭代使用的 48 位子密钥是由原始的 56 位大密钥产生的。

DES 算法加密时把明文以位为单位分成块，而后密钥把每一块明文转化成同样 64 位的密文块。DES 可提供 7.2×1016 个密钥，用每微秒可进行一次 DES 加密的机器来破译密码需 2000 年。采用 DES 的一个著名的网络安全系统是 Kerberos，由 MIT 开发，是网络通信中身份认证的工业上的事实标准。

因为对称密码系统具有加解密速度快、安全强度高等优点，在军事、外交及商业应用中使用得越来越普遍；由于存在密钥发行与管理方面的不足，在提供数字签名、身份验证等方面需要与公开密钥密码系统共同使用，以达到更好的安全效果。

1.4.3　公钥密码技术

公钥技术是在密码体制中加密和解密采用两个不同的相关的密钥的技术，又称不对称密钥技术。公钥系统的概念是 Diffie 和 Hellman 在 1976 年提出的，目前公钥算法有很多种，共同特点是每个通信方在进行保密通信时有两个相关的密钥，一个公开，另一个保密。公钥算法比传统密钥算法计算复杂度高，大量数据加密时传统加密算法的速度比公钥加密算法快 100～1000 倍，因此，公钥算法常被用来对少量关键数据(例如传统加密算法的密钥)进行加密，或者用于数字签名。常用的公钥算法有 Rivest、Shamir 和 Adleman 提出的并以他们的名字首字母命名的 RSA 算法，它可以实现加密和数字签名功能；El Gamal 和 DSS 算法实现签名但是没有加密；Diffie Hellman 算法用于建立共享密钥，没有签名也没有加密，一般与传统密码算法共同使用。这些算法复杂度各不相同，提供的功能也不完全一样。

使用最广的公钥加密算法是 RSA。RSA 使用两个密钥，一个为公共密钥，一个为专用密钥。如其中一个加密，则可用另一个解密，密钥长度从 40 位到 2048 位可变，加密时也把明文分成块，块的大小可变，但不能超过密钥的长度，RSA 算法把每一块明文转化为与密钥长度相同的密文块。密钥越长，加密效果越好，但加密、解密的开销也大，所以要在安全与性能之间折中考虑，一般 64 位是较合适的。RSA 的一个比较知名的应用是安全套接字层 SSL，在美国和加拿大 SSL 用 128 位 RSA 算法。

公共密钥的优点在于，也许你并不认识某一实体，但只要你的服务器认为该实体证书权威 CA 是可靠的，就可以进行安全通信，而这正是电子商务这样的业务所要求的，

例如信用卡购物。服务器方对自己的资源可根据客户 CA 的发行机构的可靠程度来授权。

1.5 本章小结

网络安全是在分布网络环境中,对信息载体(处理载体、存储载体、传输载体)和信息的处理、传输、存储、访问提供安全保护,以防止数据、信息内容或能力被非授权使用、篡改或拒绝服务。

网络安全的基本属性是机密性、完整性、可用性。机密性是指保证信息与信息系统不被非授权者所获取与使用,主要防范措施是密码技术。完整性是指信息是真实可信的,其发布者不被冒充,来源不被伪造,内容不被篡改,主要防范措施是校验与认证技术。可用性是指保证信息与信息系统可被授权人正常使用,主要防范措施是确保信息与信息系统处于一个可靠的运行状态之下。

国际标准化组织在开放系统互连标准中定义了 7 个层次的参考模型,不同的网络层次之间的功能基本上是不同的,相应的不同层次的网络安全服务也是不同的,需要分层进行配置。包括物理层的安全、数据链路层的加密保护、网络层的防火墙及 IP 加密、传输层的安全套接字以及在应用层针对用户身份进行认证并建立起安全的访问通道。

网络安全通用模型表示了在开放的网络环境中,保护信息的传输需要提供的安全机制和安全服务,包括实现和安全有关的转换算法,用于该算法的秘密信息的产生、分发和共享,以及确定两个主体使用的协议,以得到特定的安全服务。网络安全访问模型则考虑了黑客攻击、病毒与蠕虫等的非授权访问。

网络安全,尤其是 Internet 安全正面临着严重的挑战,主要是 Internet 规模的扩大和关键应用的激增,网络安全攻击的持续增加、安全漏洞的增长,以及网络安全的对策急需开发。

密码学是以研究数据保密为目的,对存储或传输的信息采取秘密的交换以防止第三者对信息的窃取的技术。在传统密码体制中加密和解密采用的是同一密钥,称为对称密钥密码系统,又称私钥系统。现代密码体制中加密和解密采用不同的密钥,称为非对称密钥密码系统,又称公钥系统。

习　题

1. 计算机网络是地理上分散的多台(　　)遵循约定的通信协议,通过软硬件互联的系统。

A. 计算机　　B. 主从计算机　　C. 自主计算机　　D. 数字设备

2. 网络安全是在分布网络环境中对(　　)提供安全保护。

A. 信息载体　　B. 信息的处理、传输

C. 信息的存储、访问　　D. 上面 3 项都是

3. 网络安全的基本属性是(　)。

A. 机密性　B. 可用性　C. 完整性　D. 上面 3 项都是

4. 密码学的目的是(　)。

A. 研究数据加密　B. 研究数据解密　C. 研究数据保密　D. 研究信息安全

5. 假设使用一种加密算法,它的加密方法很简单:将每一个字母加 5,即 a 加密成 f,b 加密成 g。这种算法的密钥就是 5,那么它属于(　)。

A. 对称密码技术　B. 分组密码技术

C. 公钥密码技术　D. 单向函数密码技术

6. 访问控制是指确定(　)以及实施访问权限的过程。

A. 用户权限　B. 可给予那些主体访问权利

C. 可被用户访问的资源　D. 系统是否遭受入侵

7. 一般而言,Internet 防火墙建立在一个网络的(　)。

A. 内部子网之间传送信息的中枢　B. 每个子网的内部

C. 内部网络与外部网络的交叉点　D. 部分内部网络与外部网络的接合处

8. 可信计算机系统评估准则(Trusted Computer System Evaluation Criteria,TCSEC)共分为(　)大类(　)级。

A. 4　7　B. 3　7　C. 4　5　D. 4　6

9. 橘皮书定义了 4 个安全层次,从 D 层(最低保护层)到 A 层(验证性保护层),其中 D 级的安全保护是最低的,属于 D 级的系统是不安全的,以下操作系统中属于 D 级安全的是(　)。

A. 运行非 UNIX 的 Macintosh 机　B. 运行 Linux 的 PC

C. UNIX 系统　D. XENIX

10. 计算机病毒是计算机系统中一类隐藏在(　)上蓄意破坏的捣乱程序。

A. 内存　B. 软盘　C. 存储介质　D. 网络

第2章 风险分析

本章要点：

- 资产的有效保护；
- 各种攻击的类型；
- 什么是风险；
- 如何识别风险；
- 如何测量风险。

风险分析是对需要保护的资产及其受到的潜在威胁进行鉴别的过程。而风险是威胁和漏洞(脆弱性)的组合。正确的风险分析是保证网络环境安全的极其重要的一步。

风险分析要回答以下一些问题：

- 哪些资产需要保护；
- 从哪些源来保护这些资产；
- 谁有可能危及你的网络；
- 威胁如何侵犯你的网络；
- 假如资产被危及，什么是即时的损失；
- 从攻击或失效到恢复正常需要多少花费；
- 如何能有效地、节省地保护这些资产；
- 网络环境需要的安全级别是否由主管部门确定。

2.1 资产保护

2.1.1 资产的类型

任何有效的风险分析始于需要保护的资产和资源的鉴别，资产的类型一般可分成以下4类。

(1) 物理资源

物理资源是具有物理形态的资产。包括工作站、服务器、终端、网络设备、外围设备等，基本上，凡是具有物理形态的计算资源都是物理资源。

风险分析的最终目标是制定一个有效的、节省的计划来看管资产，不要忽视显而易见的问题和解决办法。

(2) 知识资源

和物理资源相比，知识资源更难鉴别，因为它只以电子的形式存在。知识资源可以是

任何信息的形式，并且在组织的事务处理中起一定的作用。它包括软件、财务信息、数据库记录以及计划图表等。例如，公司通过电子邮件交换信息，这些电子报文的存储应看成知识资产。

（3）时间资源

时间也是一个重要的资源，甚至是一个组织最有价值的资源。当评估时间损失对一个组织的影响时，应考虑由于时间损失引起的全部后果。

（4）信誉（感觉）资源

在 2000 年 2 月，大部分网络公司诸如 Yahoo、Amazon、eBay 和 Buy. com 等在受到拒绝服务攻击以后，他们的股票价狂跌。虽然这是暂时的，但足以说明消费者和股票持有者对他们的可信度确实存在影响，且可测量。又如，2000 年 10 月围绕 Microsoft 系统的问题公开暴露，公众不仅对公司，也对其产品的可信度产生了一定的影响。

2.1.2　潜在的攻击源

潜在的网络攻击可来自任何能访问网络的源，这些源之间有很大差异，它依赖于一个组织的规模以及提供的网络访问的类型。当作风险分析时，要能识别所有的攻击源。这些攻击源包括内部系统、来自办公室的访问、通过广域网联到经营伙伴的访问、通过 Internet 的访问，以及通过 modem 池的访问等。

在分析潜在攻击源时不仅要评估谁可能攻击网络，还要寻找什么样的介质可用来对网络资源的访问。

潜在的攻击来自多方面，包括组织内部的员工、临时员工和顾问、竞争者和组织中具有不同观点和目的的人、反对这个组织或其员工的人。根据这个组织的情况，还可能有各种不同的攻击源。重要的是要决定什么样的威胁能实现成功的攻击，以及对潜伏的攻击者而言，什么样的攻击是值得的。

在识别资源以及潜在的攻击源后，可评估该组织受攻击的潜在风险级别。一个网络是物理隔离的网，还是有很多入口（如广域网）、有 modem 池，或是经过 Internet 进入的 VPN？所有这些连接点是否使用强的身份鉴别和某种形式的防火墙设备，或者其他的网络保护措施？攻击者能否发现某一个暴露的访问点以及获得访问该网络资源？

对攻击可能性的看法在很大程度上是带有主观性的，同一个组织的两个人对攻击可能性的观点可能完全不同。因此要听取来自不同部门的观点，甚至聘请在决定风险评估方面有实践经验的顾问。因为对攻击可能性的分析越清楚，越能更有效地保护网络。

2.1.3　资产的有效保护

资产一旦受到威胁和破坏，就会带来两类损失，一类是即时的损失，如由于系统被破坏，员工无法使用，因而降低了劳动生产率；又如，ISP 的在线服务中断带来经济上的损失。另一类是长期的恢复所需花费，也就是从攻击或失效到恢复正常需要的花费，例如，受到拒绝服务攻击，在一定期间内资源无法访问带来的损失；又如，为了修复受破坏的关键文件所需的花费等。

为了有效保护资产，应尽可能降低资产受危害的潜在代价。另外，由于采取一些安全

措施，也要付出安全的操作代价。网络安全最终是一个折中的方案，需要对危害和降低危害的代价进行权衡。

在评估时要考虑网络的现有环境，以及近期和远期网络发展变化的趋势。选用先进的安全体系结构和系统安全平台可减少安全操作代价，获得良好的安全强度。

除此之外，要获得安全强度和安全代价的折中，需要考虑以下因素：

(1) 用户的方便程度。不应由于增加安全强度给用户带来很多麻烦。

(2) 管理的复杂性。对增加安全强度的网络系统要易于配置、管理。

(3) 对现有系统的影响。包括增加的性能开销以及对原有环境的改变等。

(4) 对不同平台的支持。网络安全系统应能适应不同平台的异构环境的使用。

图 2-1 所示为安全强度和安全代价的折中，其中图 2-1(a)表示安全强度和安全操作代价的关系。图 2-1(b)表示安全强度和侵入系统可能性的关系。图 2-1(c)表示将图 2-1(a)和图 2-1(b)合在一起，其相交点是平衡点，即安全强度和安全代价的折中选择。图 2-1(d)表示由于入侵手段增强引起的变化，从而产生新的平衡点。

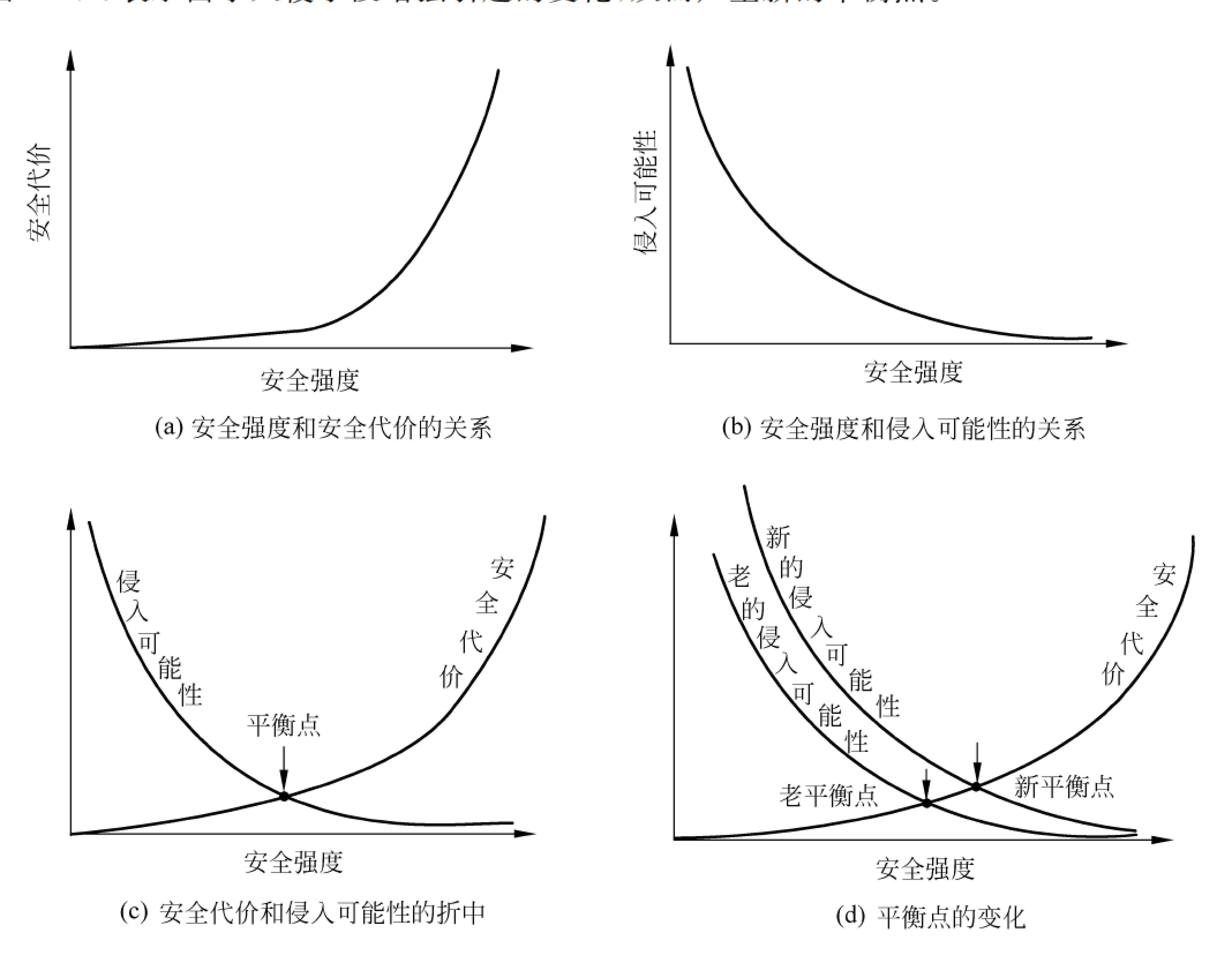


图 2-1　安全强度和安全代价的折中

为了有效保护资产，需要一个性能良好的安全系统结构和安全系统平台，可以小的安全代价换取高的安全强度。

2.2 攻击

221 攻击的类型

从安全属性来看,攻击类型可分为以下 4 类,如图 2-2 所示,图 2-2(a)是从源站到目的站的正常信息流。

(1) 阻断攻击

阻断攻击使系统的资产被破坏,无法提供用户使用,这是一种针对可用性的攻击,如图 2-2(b)所示。例如,破坏硬盘之类的硬件,切断通信线路,使文件管理系统失效等。

(2) 截取攻击

截取攻击可使非授权者得到资产的访问,这是一种针对机密性的攻击,如图 2-2(c)所示。非授权者可以是一个人、一个程序或一台计算机,例如,通过窃听获取网上数据及非授权的复制文件和程序。

(3) 篡改攻击

篡改攻击是非授权者不仅访问资产,而且能修改信息,这是一种针对完整性的攻击,如图 2-2(d)所示。例如,改变数据文件的值、修改程序及在网上正在传送的报文内容。

(4) 伪造攻击

伪造攻击是非授权者在系统中插入伪造的信息,这是一种针对真实性的攻击,如图 2-2(e)所示。例如,在网上插入伪造的报文,或在文件中加入一些记录。

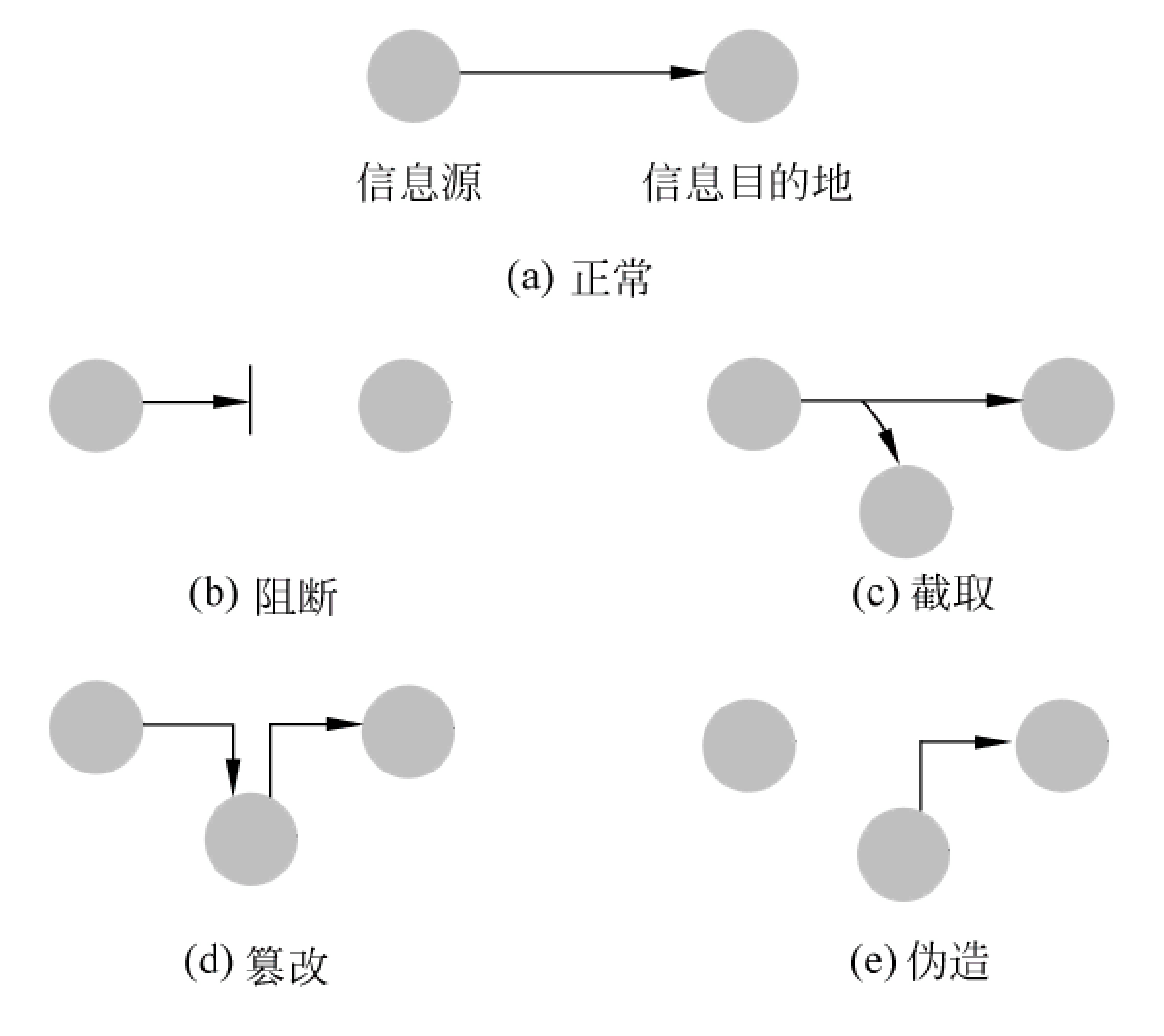


图 2-2　各种安全威胁

222 主动攻击和被动攻击

从攻击方式来看,攻击类型可分为被动攻击和主动攻击,如图 2-3 所示。

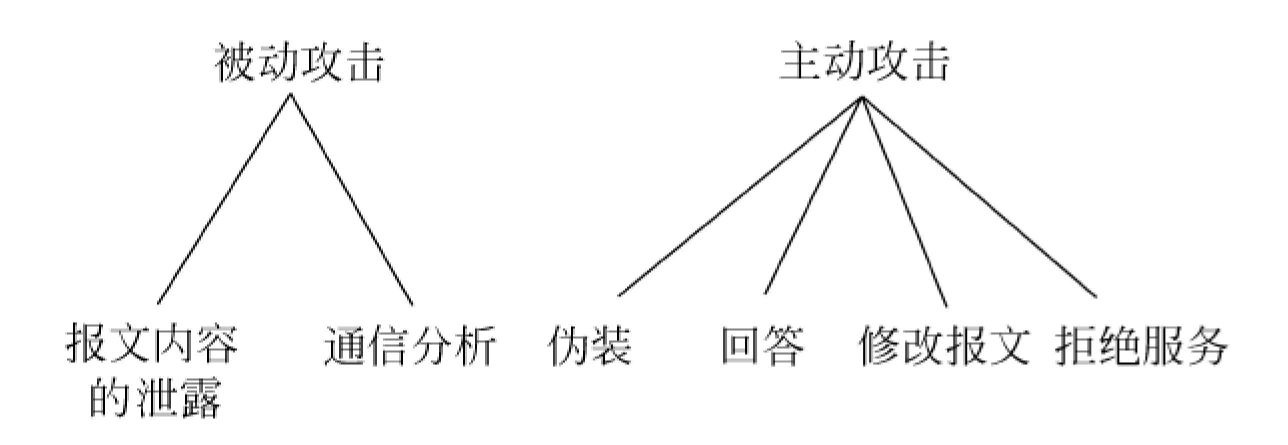


图 2-3　主动和被动安全威胁

1. 被动攻击

窃听、监听都具有被动攻击的本性，攻击者的目的是获取正在传输的信息。被动攻击包括传输报文内容的泄露和通信流量分析。报文内容的泄露易于理解，一次电话通信、一份电子邮件报文、正在传送的文件都可能包含敏感信息或秘密信息。为此要防止对手获悉这些传输的内容。

通信流量分析的攻击较难捉摸。假如有一个方法可屏蔽报文内容或其他信息通信，那么即使这些内容被截获，也无法从这些报文中获得信息。最常用的屏蔽内容技术是加密。然而即使用加密保护内容，攻击者仍有可能观察到这些传输的报文形式。攻击者有可能确定通信主机的位置和标识，也可能观察到正在交换的报文频度和长度。而这些信息对猜测正在发生的通信特性是有用的。

对被动攻击的检测十分困难，因为攻击并不涉及数据的任何改变。然而阻止这些攻击的成功是可行的，因此，对被动攻击强调的是阻止而不是检测。

2 主动攻击

主动攻击包含对数据流的某些修改，或者生成一个假的数据流。它可分成 4 类：

(1) 伪装

伪装是一个实体假装成另一个实体。伪装攻击往往连同另一类主动攻击一起进行。例如，身份鉴别的序列被捕获，并在有效的身份鉴别发生时作出回答，有可能使具有很少特权的实体得到额外的特权，这样不具有这些特权的人获得了这些特权。

(2) 回答(重放)

回答攻击包含数据单元的被动捕获，随之再重传这些数据，从而产生一个非授权的效果。

(3) 修改报文

修改报文攻击意味着合法报文的某些部分已被修改，或者报文的延迟和重新排序，从而产生非授权的效果。

(4) 拒绝服务

拒绝服务攻击是阻止或禁止通信设施的正常使用和管理。这种攻击可能针对专门的目标(如安全审计服务)，抑制所有报文直接送到目的站；也可能破坏整个网络，使网络不可用或网络超负荷，从而降低网络性能。

主动攻击和被动攻击具有相反的特性。被动攻击难以检测出来，然而有阻止其成功的方法。而主动攻击难以绝对地阻止，因为要做到这些，就要对所有通信设施、通路在任何时间进行完全的保护。因此，对主动攻击采取检测的方法，并从破坏中恢复。因为制止

的效应也可能对防止破坏做出贡献。

223　访问攻击

访问攻击是攻击者企图获得非授权信息，这种攻击可能发生在信息驻留在计算机系统中或在网络上传输的情况下，如图 2-4 所示。这类攻击是针对信息机密性的攻击。

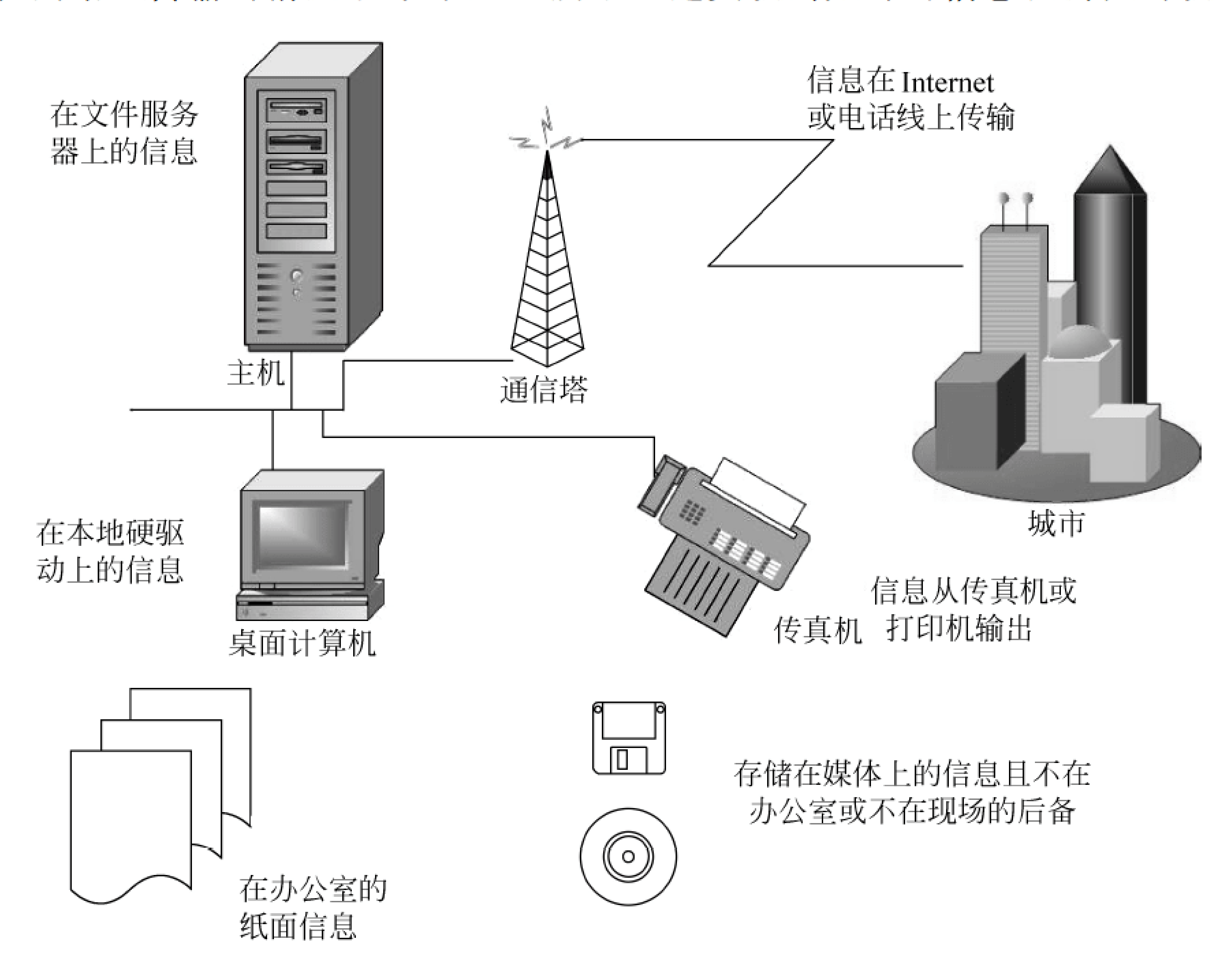


图 2-4　访问攻击可能发生的地方

常见的访问攻击有 3 种：

(1) 窥探

窥探(snooping)是查信息文件，发现某些对攻击者感兴趣的信息。攻击者试图打开计算机系统的文件，直到找到所需信息。

(2) 窃听

窃听(eavesdropping)是偷听他人的对话，为了得到非授权的信息访问，攻击者必须将自己放在一个信息通过的地方，一般采用电子的窃听方式，如图 2-5 所示。

(3) 截获

截获(interception)不同于窃听，它是一种主动攻击方式。攻击者截获信息是通过将自己插入信息通过的通路，且在信息到达目的地前能事先捕获这些信息。攻击者检查截获的信息，并决定是否将信息送往目的站，如图 2-6 所示。

电子信息可存储在桌面计算机、服务器、笔记本计算机、软盘、U 盘、CD-ROM 及后备磁带中。如没有物理安全措施，这些介质可能被偷走，攻击者就很容易得到所要的信息。

如果攻击者设法取得合法访问权，就可简单地打开文件系统。假如访问控制权限设置恰当，系统就可对非授权者拒绝访问。正确的许可权设置可阻止大部分不经心的窥视。

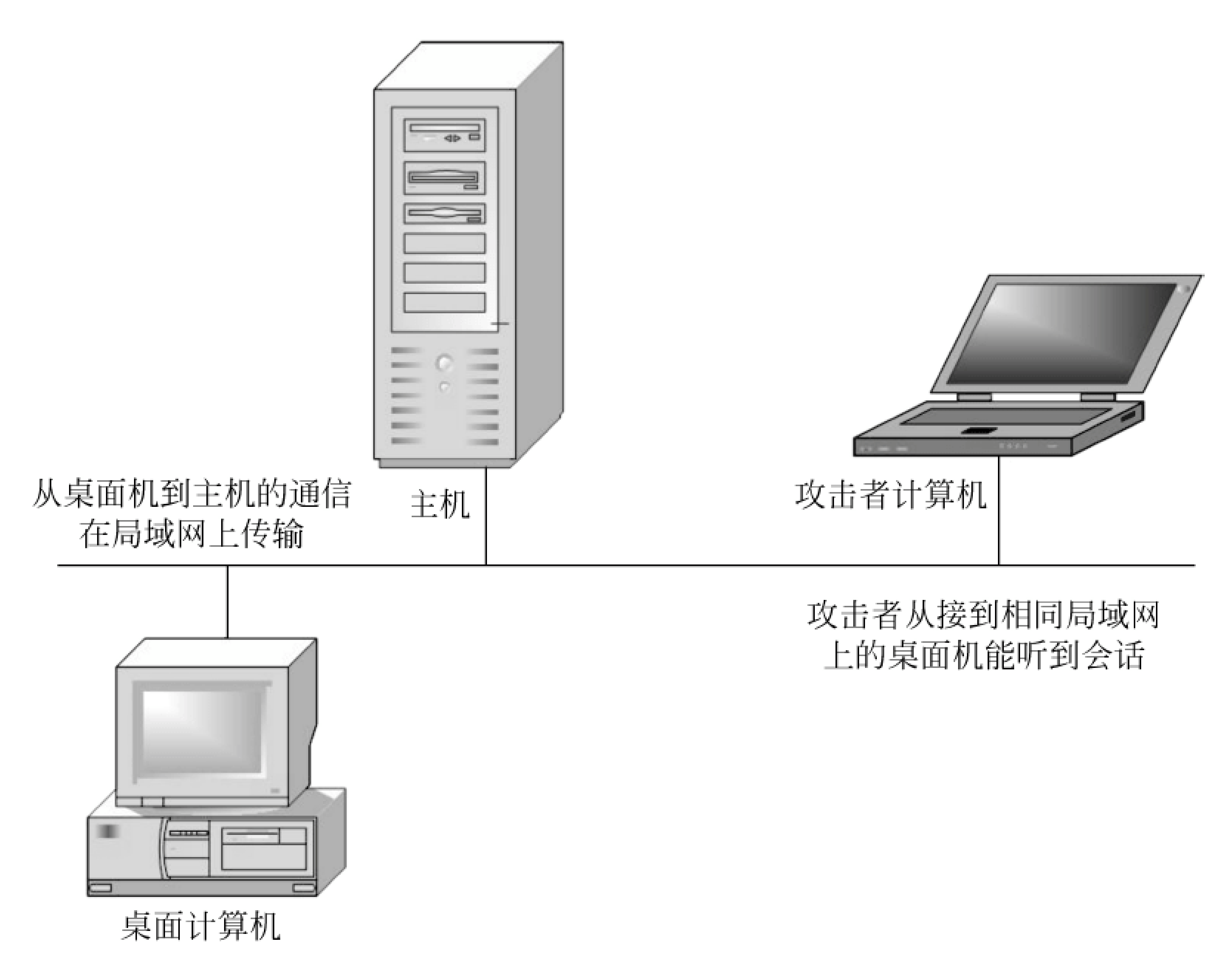


图 2-5　窃听

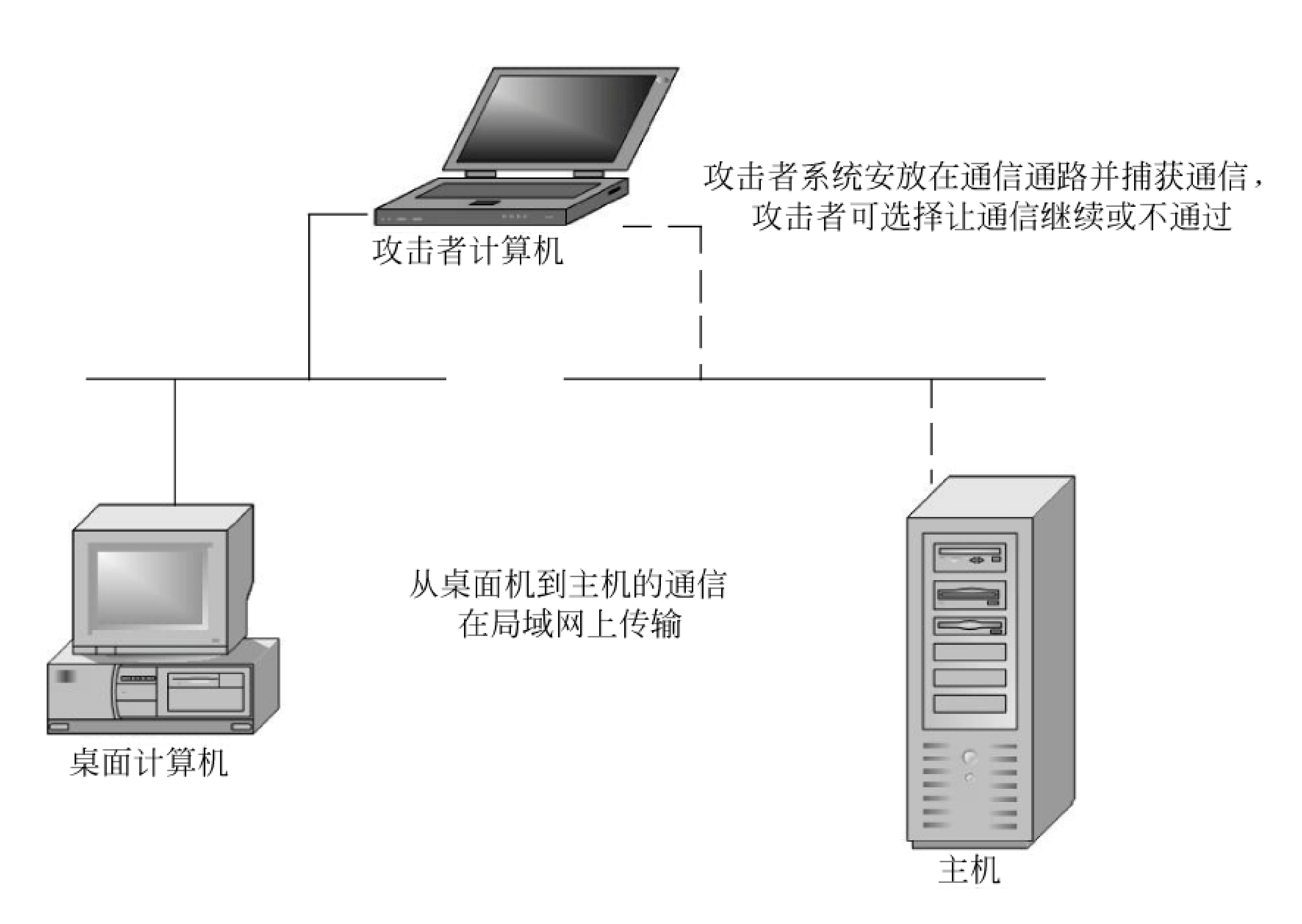


图 2-6　截获

然而对有意的攻击者企图偷到许可权，并阅读文件或降低对文件访问的控制，由于系统有很多漏洞，使得攻击者的这些行动能得逞。

对传输中的信息可通过窃听获得。在局域网中，攻击者在联到网上的计算机系统中安装一个信息包探测程序(sniffer)，来捕获在网上的所有通信。通常配置成能捕获 ID 和口令。

窃听也可能发生在广域网(如租用线和电话线)中，然而这类窃听需要更多的技术和设备。通常在设施的接线架上采用 T 形分接头来窃听信息。它不仅用于电缆线，也可用

于光纤传输线，但需要专门的设备。

使用截获来取得所需信息，对攻击者来说也比较困难。攻击者必须将自己的系统插入到发送站和接收站之间。在 Internet 上，可通过名字转换的改变来达到目的，即将计算机名转换成一个错误的 IP 地址，如图 2-7 所示。这样信息就送到攻击者的系统，而不是正确的目的站。如果攻击者正确地配置其系统，发送者和目的站可能永远不知道他是在和攻击者通信。

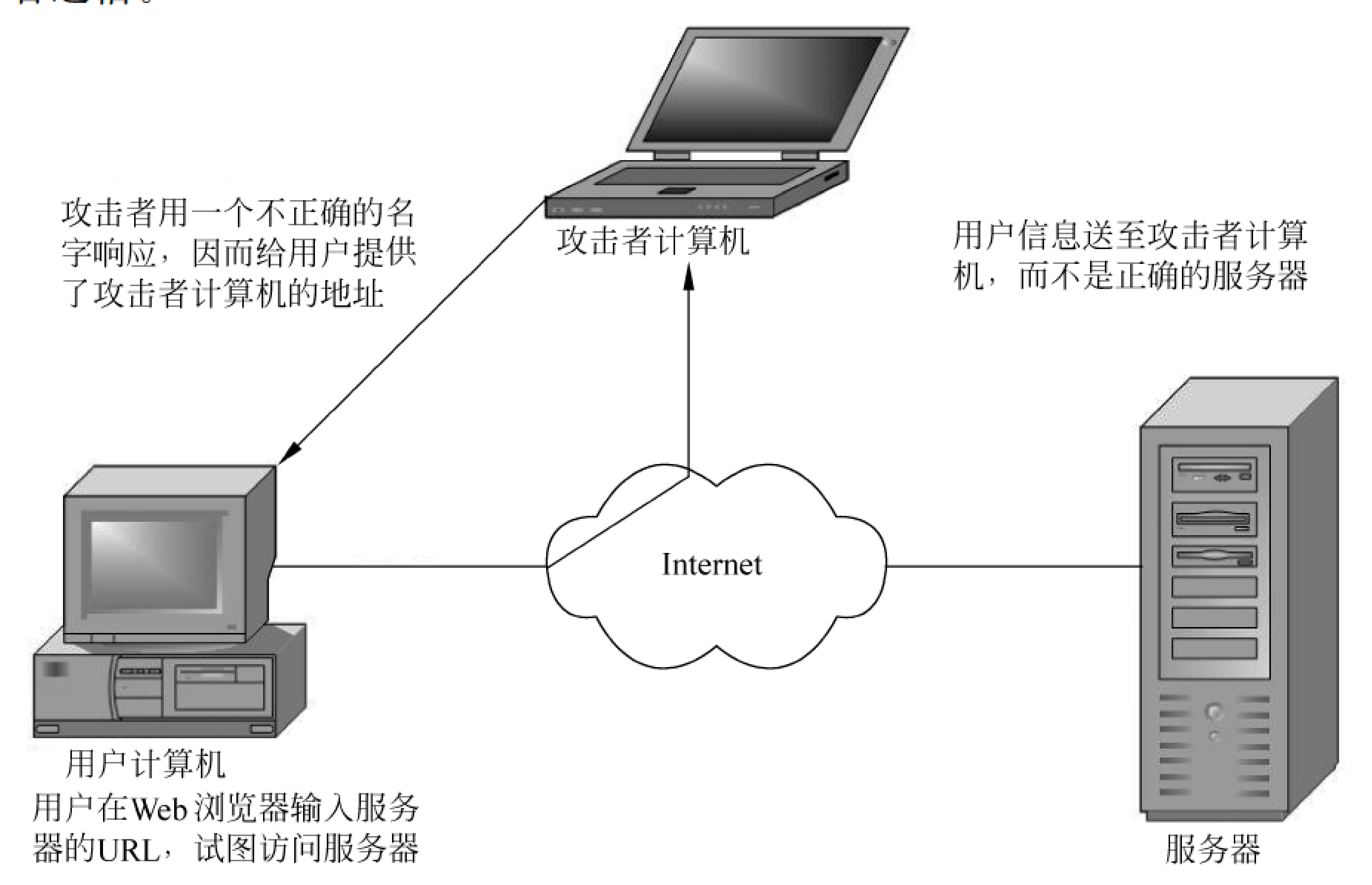


图 2-7　使用错误的名字转换截获信息

截获还可对已经进行的正常会话接管和转移。这类攻击发生在交互式通信中，如 telnet。这时，攻击者必须在客户机或服务器的同一网段。攻击者让合法用户开始和服务器会话，然后使用专门的软件来接管这个会话。这类攻击使攻击者能在服务器上具有同样的特权。

224　篡改攻击

篡改攻击是攻击者企图修改信息，而他们本来是无权修改的。这种攻击可能发生在信息驻留在计算机系统中或在网络上传输的情况下，是针对信息完整性的攻击。

常见的篡改攻击有 3 种：

(1) 改变

改变已有的信息。例如，攻击者改变已存在的员工工资，改变以后的信息虽然仍存在于该组织，但已经是不正确的信息。这种改变攻击的目标通常是敏感信息或公共信息。

(2) 插入

插入信息可以改变历史的信息。例如，攻击者在银行系统中加一个事务处理，从而将客户账户的资金转到自己账户上。

(3) 删除

删除攻击是将已有的信息去除，可能是将历史记录的信息删除。例如，攻击者将一个事务处理记录从银行结账单中删除，从而造成银行资金的损失。

修改电子信息比修改纸上信息容易得多。假如攻击者已经访问了文件,可以几乎不留证据地修改。假如攻击者没有访问文件的权限,则攻击者首先必须提高对系统的访问权,或者移去文件的许可权。在访问攻击中,攻击者利用系统的漏洞获取访问权,然后再修改文件。

攻击者要改变数据库文件或处理队列更难一些。在某些情况下,事务处理也编成序列号,不正确地移走或加一个序列号,会导致系统发出警报。只有对整个系统进行变更,才能使篡改不易被察觉。

225　拒绝服务攻击

拒绝服务攻击(Denial-of-Service, DoS)是拒绝合法用户使用系统、信息、能力等各种资源。拒绝服务攻击一般不允许攻击者访问或修改计算机系统的信息。拒绝服务攻击可分成以下 4 种:

(1) 拒绝访问信息

拒绝访问信息使信息不可用,不论是信息被破坏或者将信息改变成不可使用状态,也可能信息仍存在,但已经被移到不可访问的位置。

(2) 拒绝访问应用

拒绝访问应用的目标是操纵或显示信息的应用。通常对正在运行应用程序的计算机系统进行攻击,这样应用程序不可用,以致不能执行由该应用程序完成的任务。

(3) 拒绝访问系统

拒绝访问系统通常是使系统宕机,使运行在该计算机系统上的所有应用无法运行,使存储在该计算机系统上的所有信息不可用。

(4) 拒绝访问通信

拒绝访问通信是针对通信的一种攻击,已有很多年历史。这类攻击可能用切断通信电缆、干扰无线电通信以及用过量的通信负载来淹没网络。拒绝访问通信的目标是通信介质本身,从而阻止用户通过网络访问系统和信息。

拒绝服务攻击主要是针对计算机和网络系统。

很多方法可以使电子形式的信息遭受拒绝服务攻击。在拒绝访问信息的同时,信息有可能被删除,当然这类攻击需要同时将后备信息也删除。也有可能通过改变文件提供无用信息,例如,攻击者对文件加密并毁掉密钥,这样任何人都无法访问这些信息。

带有信息的计算机也可能被偷走。短期的拒绝服务攻击可以简单地将系统关掉,导致系统本身拒绝服务。拒绝服务攻击可直接针对系统,使计算机系统破坏。

通过一些漏洞可使应用程序不可用。这类漏洞使攻击者对应用程序发送一些事先设定的命令,从而使应用程序无法正常运行。应用程序看起来像被摧垮一样,即使重新启动,仍无法运行。

最容易使通信设施不可用的方法是切断电缆。但这类攻击需要到现场物理访问网络电缆。另一种拒绝服务攻击的方法是对一个场地发送大量的通信量,阻止合法用户使用。

226　否认攻击

否认攻击是针对信息的可审性进行的。否认攻击企图给出假的信息或者否认已经发

生的现实事件或事务处理。

否认攻击包括两类：

（1）假冒

假冒是攻击者企图装扮或假冒别人和别的系统。这种攻击可能发生在个人通信、事务处理或系统对系统的通信中。

（2）否认

否认一个事件是简单地抵赖曾经登录和处理的事件。例如，一个人用信用卡在商店里购物，然而当账单送到时，告诉信用卡公司，他从未到该商店购物。

电子信息比纸上信息更易实现否认攻击。电子文本能生成和发送给别人，而几乎没有发送者身份的证据。例如，发送者发送电子邮件，可以任意改变其发送者地址，电子邮件系统几乎不能验证发送者的身份。

同样地，网上计算机系统发送信息时，可用任何 IP 地址，这样的计算机系统就可伪装成另一个系统。

2.3　风险管理

从本质上讲，安全就是风险管理。一个组织者如果不了解其信息资产的安全风险，很多资源就会被错误地使用。风险管理提供信息资产评估的基础。通过风险识别，可以知道一些特殊类型的资产价值以及包含这些信息的系统的价值。

2.3.1　风险的概念

风险是构成安全基础的基本观念。风险是丢失需要保护的资产的可能性。如果没有风险，就不需要安全了。风险还是从事安全产业者应了解的一个观念。

以传统的保险业为例来了解风险的含义。一个客户因感到危险，所以向保险公司购买保险。买保险前，如果出车祸，他需要花很多修理费，买了保险后就可减少花大笔钱的风险。保险公司设定保险费的依据有两个，一个是汽车修理的费用，另一个是该客户发生车祸的可能性。

从上面的例子可以看出，风险包含两个部分。第一个是车的修理费，如果车祸发生，保险公司就要付这笔费用，将它定为保险公司的漏洞或脆弱性。第二个是客户发生车祸的可能性，这是对保险公司的威胁，因为它有可能使保险公司付修理费。因此，漏洞和威胁是测定风险的两个组成部分。图 2-8 表示漏洞和威胁之间的关系，由图可知，如果没有威胁，也就没有风险；同样地，如果没有漏洞，也就没有风险。

1. 漏洞

漏洞是攻击的可能的途径。漏洞有可能存在于计算机系统和网络中，它允许打开系统，使技术攻击得逞。漏洞也有可能存在于管理过程中，它使系统环境对攻击开放。

漏洞的多少是由需要打开系统的技术熟练水平和困难程度来确定的，还要考虑系统暴露的后果。如果漏洞易于暴露，并且一旦受到攻击，攻击者可以完全控制系统，则称高

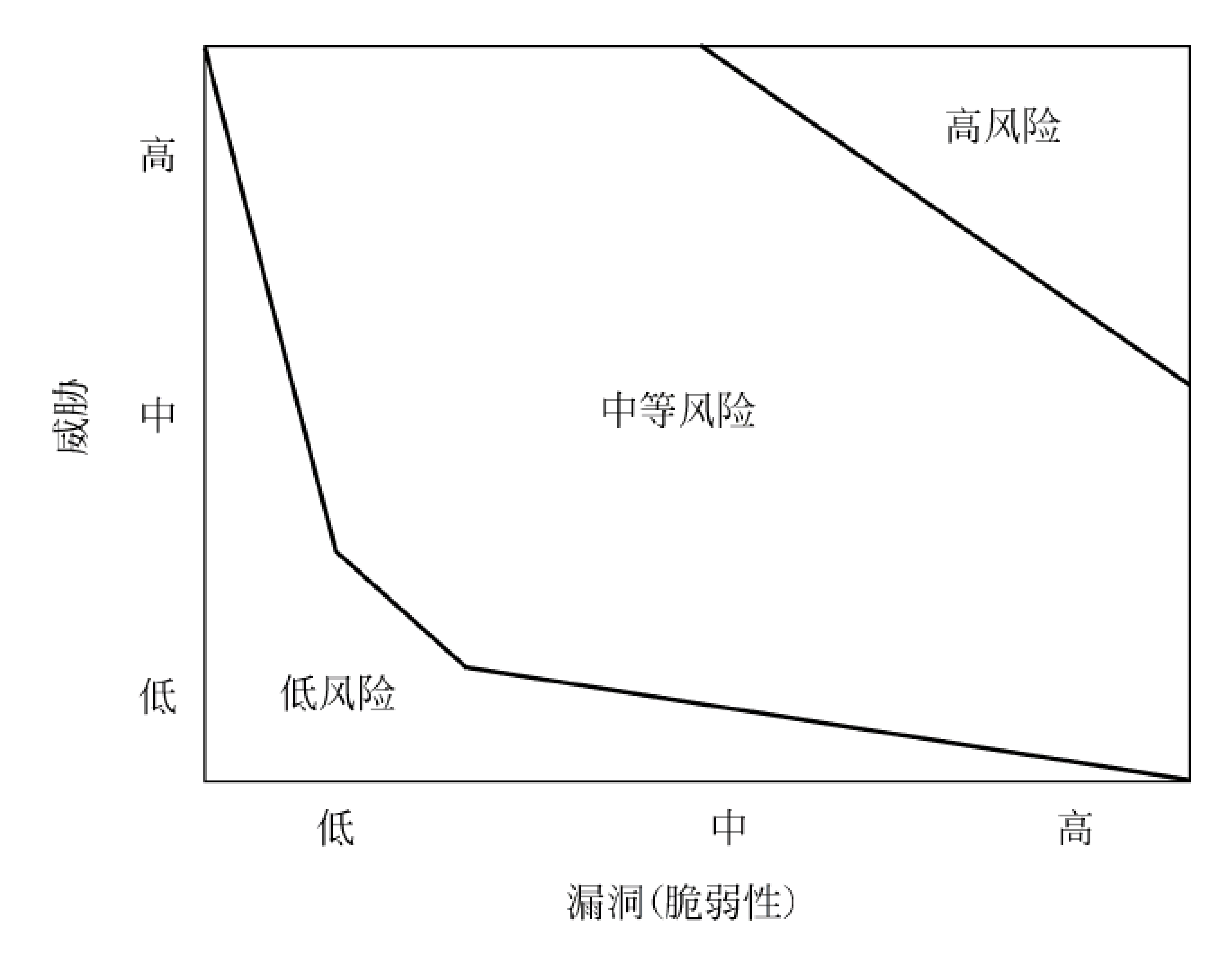


图 2-8　漏洞和威胁的关系

值漏洞或高脆弱性。如果攻击者需要对设备和人员投入很多资源,漏洞才能暴露,并且受到攻击后,也只能获取一般信息,而非敏感信息,则称低值漏洞或低脆弱性。

漏洞不仅和计算机系统、网络有关,而且和物理场地安全、员工的情况、传送中的信息安全等有关。

2 威胁

威胁是一个可能破坏信息系统环境安全的动作或事件。威胁包含以下 3 个组成部分:

(1) 目标

威胁的目标通常是针对安全属性或安全服务,包括机密性、完整性、可用性、可审性等。这些目标是在威胁背后的真正理由或动机。一个威胁可能有几个目标,例如,可审性可能是攻击的首要目标,这样可防止留下攻击者的记录,然后,把机密性作为攻击目标,以获取一些关键数据。

(2) 代理(攻击主体)

代理需要有 3 个特性:

- 访问。一个代理必须有访问所需要的系统、网络、设施或信息的能力。可以是直接访问,例如,代理有系统的账号。也可以是间接访问,例如,代理通过其他的方法来访问系统。代理有的访问直接影响到为了打开漏洞所必须执行的动作的能力。
- 知识。一个代理必须具有目标的知识,有用的知识包括用户 ID、口令、文件位置、物理访问过程、员工的名字、访问电话号码、网络地址、安全程序等。代理对目标越熟悉,就具有越多的存在的漏洞的知识;代理对存在的漏洞知道得越具体,就越能获得更多打开漏洞的知识。
- 动机。一个代理对目标发出威胁,需要有动机,通常动机是考虑代理攻击目标的

关键特性。动机可能是不同的，有的为了竞争、挑战；有的是贪心，以获得钱、物、服务、信心；有的是对某组织或个人有恶意伤害的企图。

根据代理的 3 个特性，应该考虑的代理可能是各种各样的，包括员工、和组织有关的外部员工、黑客、商业对手、恐怖分子、罪犯、客户、访问者及自然灾害等。

当考虑这些代理时，应该作出定量的判断，以得出每个代理对访问组织的目标的必要性，根据前面分析的漏洞考虑攻击的可能性。

(3) 事件(攻击行为)

事件是代理采取的行为，从而导致对组织的伤害。例如，一个黑客改变一个组织的 Web 页面来伤害它。另外要考虑的是假如代理得到访问会产生什么样的伤害。

常见的事件如下：

- 对信息、系统、场地滥用授权访问；
- 恶意地改变信息；
- 偶然地改变信息；
- 对信息、系统、场地非授权访问；
- 恶意地破坏信息、系统、场地；
- 偶然地破坏信息、系统、场地；
- 对系统和操作的恶意物理损害；
- 对系统和操作的偶然物理损害；
- 由于自然物理事件引起的系统和操作的损害；
- 引入对系统的恶意软件；
- 破坏内部或外部的通信；
- 被动地窃听内部或外部的通信；
- 偷窃硬件。

3. 威胁＋漏洞＝风险

风险是威胁和漏洞的综合结果。没有漏洞的威胁没有风险，没有威胁的漏洞也没有风险。风险的度量是要确定事件发生的可能性和造成的损失。风险可划分成低、中、高 3 个级别。

(1) 低级别风险是漏洞使组织的风险达到一定水平，然而不一定发生。如有可能应将这些漏洞去除，但应权衡去除漏洞的代价和能减少的风险损失。

(2) 中级别风险是漏洞使组织的信息系统或场地的风险(机密性、完整性、可用性、可审性)达到相当的水平，并且已有发生事件的现实可能性。应采取措施去除漏洞。

(3) 高级别风险是漏洞对组织的信息、系统或场地的机密性、完整性、可用性和可审性已构成现实危害。必须立即采取措施去除漏洞。

2.3.2　风险识别

对一个组织而言，识别风险除了要识别漏洞和威胁外，还应考虑已有的对策和预防措施，如图 2-9 所示。

1. 识别漏洞

识别漏洞时，从确定对该组织的所有入口开始，也就是寻找该组织内的系统和信息的

所有访问点。这些入口包括 Internet 的连接、远程访问点、与其他组织的连接、设备的物理访问及用户访问点等。

对每个访问点识别可访问的信息和系统，然后识别如何通过入口访问这些信息和系统。应该包括操作系统和应用程序中所有已知的漏洞。在以后的章节里还会详细地作风险评估。

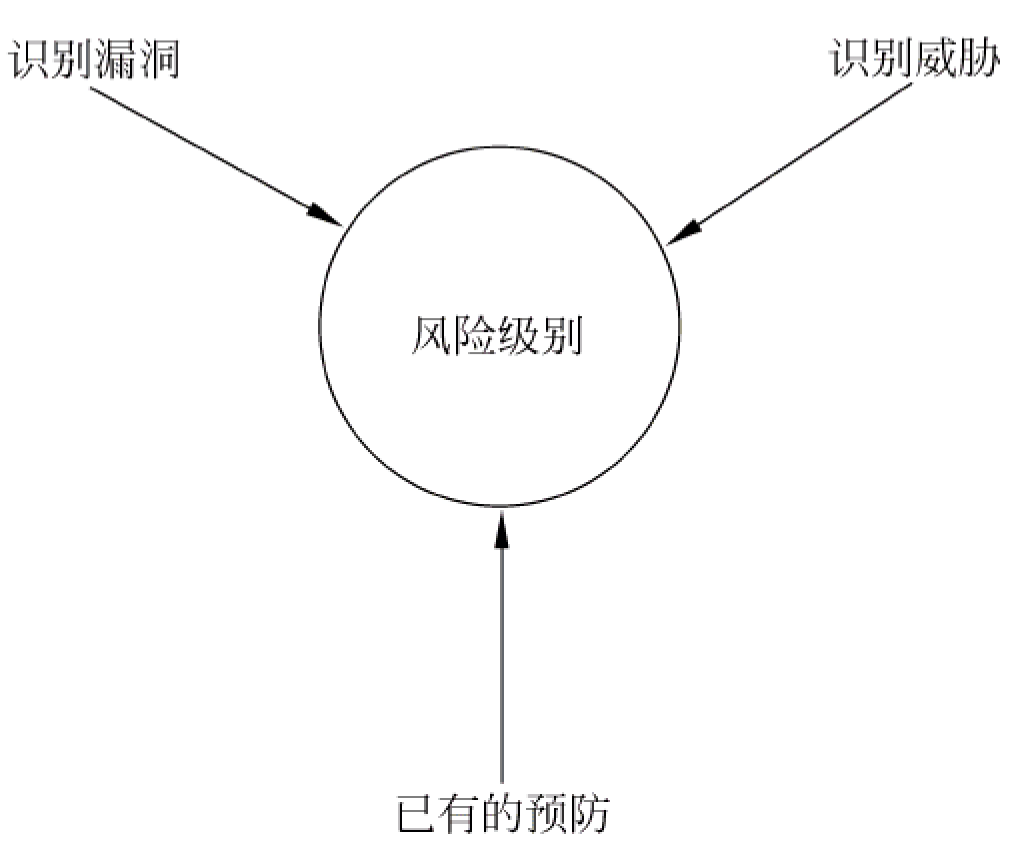


图 2-9　一个组织风险评估的组成

2 识别现实的威胁

威胁评估是十分具体的，有时也是很困难的。在试图识别一个组织或目标的威胁时，经常会转到那些竞争对手的身上。然而，真正的威胁往往是非常隐蔽的，在攻击事件发生以前，真正的目标威胁往往并不暴露出来。

一个目标威胁是对一个已知的目标具有已知的代理、已知的动机、已知的访问和执行已知的事件的组合。例如，有一个不满意的员工（代理）希望得到正在该组织进行的最新设计的知识（动机），该员工能访问组织的信息系统（访问），并知道信息存放的位置（知识）。该员工正窥测新设计的机密并且企图获得所需文件。

识别所有的目标威胁是非常费时和困难的。可以变更一种方法，即假设存在一个威胁的通用水平，这个威胁可能包括任何具有访问组织信息或系统的可能性的人。这个威胁确实是存在的，因为人们（员工、客户、供应商等）必须访问该组织的系统和信息，这对其工作是有用的。然而，我们不必要具有对组织某些部分的直接的或特定的威胁的知识。

假如我们假设一个通用的威胁（某些人可能具有访问、知识、动机做某些坏事），就能检查组织内允许这些访问发生可能产生的漏洞。将任何这样的漏洞计入风险，因为我们已经假定这些有可能暴露漏洞的威胁。

3. 检查对策和预防措施

在分析评估攻击的可能途径时，必须同时检查如果漏洞真正存在，相应环境采取的对策和预防措施。这些预防措施包括防火墙、防病毒软件、访问控制、双因子身份鉴别系统、仿生网络安全程序、用于访问设备的卡读出器、文件访问控制、对员工进行安全培训等。

对于组织内的每个访问点都应有相应的预防措施。例如，该组织有一个 Internet 连接，这就提供了访问该组织内部系统的可能性。可以采用防火墙来保护这个访问点，设置和检查防火墙的规则，可以很好地识别来自外部对内部系统访问的企图。这样外部攻击者不能用访问点的某些漏洞，因为防火墙阻止访问这些漏洞和系统。

4. 识别风险

一旦对漏洞、威胁、预防措施进行了识别，就可确定该组织的风险。问题变得简单了，即给出具有已存在的预防措施下识别的访问点，还有可能进入该组织的访问点。

为了回答这个问题，首先确定每个访问点的可能威胁或通用威胁，并检查通过每个访问点的可能的目标（机密性、完整性、可用性、可审性）。基于它的危险程度给每个风险分成高、中、低等级。必须指出，对于相同的漏洞，可能得出基于访问点的不同级别的风险。例如，一个内部系统在它的邮件系统内有一个漏洞，对外部来说，攻击者必须通过Internet 防火墙才能发现系统，这样通过该访问点，系统是不可访问的，因此没有风险。然而，对内部员工而言，他们无须通过防火墙进入网络，因而可访问系统。这就意味着内部员工可以利用这个漏洞来访问系统，而内部员工并未列为威胁源，因此可将它列为中等风险级别。

上述例子中，如果物理安全控制很弱，任何人可随意进出，使非授权者可操作该系统，则该系统即使有防火墙这类预防措施，对具有恶意动机的攻击者来说也是无效的。由于缺乏物理安全预防措施，这种情况下应列为高风险级别。

当然，仅仅将风险分成高、中、低 3 个级别还未解决风险识别的全部问题，还应看如果漏洞暴露，对该组织的危害是否是持续的；该组织需要花费多少资源，才能减少风险。

2.3.3　风险测量

风险测量必须识别出在受到攻击后该组织需要付出的代价。图 2-10 表示风险测量的全部。

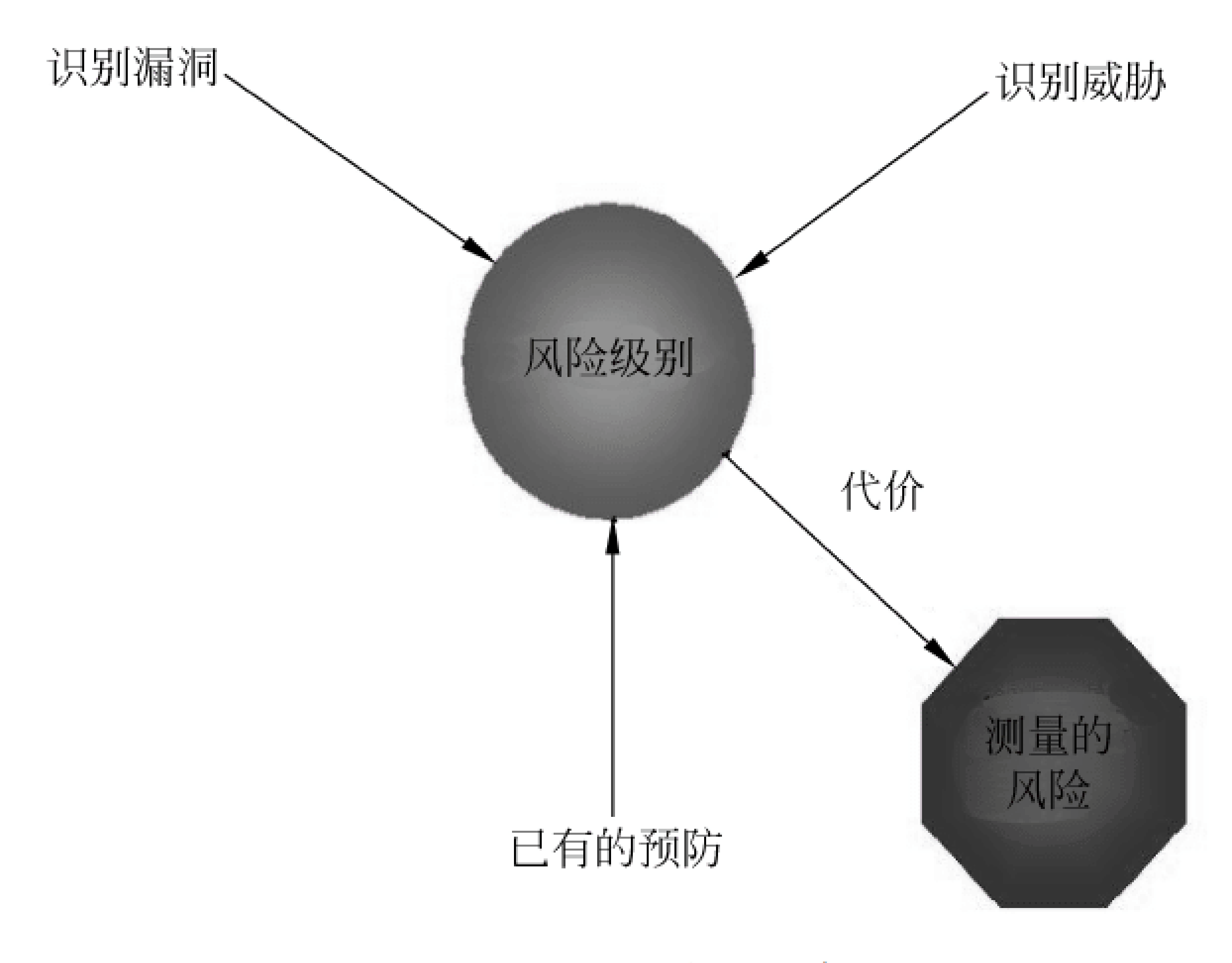


图 2-10　测量风险

认识到风险使该组织付出的代价也是确定如何管理风险的决定因素。风险永远不可能完全去除，风险必须管理。

代价是多方面的，包括资金、时间、资源、信誉及丢失生意等。

1. 资金

资金是最显而易见的风险代价，包括损失的生产能力、设备或金钱的被窃、调研的费用、修理或替换系统的费用、专家费用、员工加班时间等。

上面只是列出了部分代价，可见风险代价之巨大。有些损失在实际的事件发生前是

不知道的，也应将其计入风险代价。

最困难的资金代价估计是损失的生产能力这一项。有的生产能力损失是永远不可恢复的，有的生产能力损失可在付出一定费用恢复系统后恢复。有些是难以估计的，例如，在一个制造工厂，它依靠计算机系统调度生产、预订原料、跟踪生产流程，如受到攻击后，系统不可用了，有可能使 24 小时后原材料供应不上了，而调度生产在一个 8 小时班后也停了。设想一下，如果计算机系统 7 天不可用，这时该工厂的损失有多大，需要计及这 7 天停工的损失，及为使生产恢复正常需要加班的时间，甚至还有一些不可估计的损失。

2. 时间

时间的代价很难量化。由于安全事件使一个技术人员不能执行其正常的任务，或许可以按时间的总和计算，但又如何计算其他人员等待计算机修复所付出的时间代价呢？

时间可能以关键系统宕机时间来计算，例如，一个组织的 Web 站受破坏了，该系统只能离线并修复。那么如何计算该 Web 站宕机所造成的影响？

再如，由于攻击得逞导致该组织的产品延迟，如何来计算由于该延迟引起的损失，但无论如何，时间损失必须计入风险测量中。

3. 资源

资源可以是人、系统、通信线路、应用程序或访问。资源代价指如攻击得逞，需要多少资源来恢复正常。很明显，对一些能用钱来计算的资源是可能计算的，然而对一些不可用钱来计算的资源就难以估算，如本应去完成另一任务的人来处理该事故恢复，则另一任务的延误如何确定其代价？ 又如，攻击使网络连接很慢，由此引起的很多需要连接网络的工作延误，这一损失代价又如何计算？

4. 信誉

一个组织的信誉损失是十分关键的损失，然而这类损失的代价也难以测量。什么是一个组织的真正的信誉损失代价？

信誉就是诚信、可信。一个组织在公众心目中的可信度是十分重要的。例如，银行的信誉就等于该银行在公众心目中的可信度，客户的钱是否能安全地存放决定了客户是否愿意将钱存入该银行，否则客户就会将已存的钱从该银行取走，甚至使银行倒闭。又如，一个慈善机构的信誉就是能否合理地使用捐款，这决定了它是否能募集到资金。

对每个识别风险的风险测量的可能结果，回答以下问题：

- 识破风险所需的花费是多少？ 包括跟踪的员工时间、顾问时间、新设备的花费。
- 为了成功地识破风险要花多少时间？
- 什么样的资源会受到影响？ 而组织的哪一部分依赖于这些资源？
- 该事件对组织的信誉影响如何？
- 会丢失多少经营的业务？ 什么类型的业务会丢失？

回答了上述问题以后，可列出一个表，以表示每个风险可能引起的后果。利用这些信

息来开发相应的风险管理项目。

2.4 本章小结

风险分析是对需要保护的资产及其受到的潜在威胁的鉴别过程。风险是威胁和漏洞的组合。正确的风险分析是保证网络环境及其信息安全的极其重要的一步。

风险分析始于对需要保护的资产(物理资源、知识资源、时间资源、信誉资源)的鉴别及对资产威胁的潜在攻击源的分析。资产的有效保护是尽可能降低资产受危害的潜在代价及由于采取安全措施付出的操作代价。一个性能良好的安全系统结构和安全系统平台,可以低的安全代价换取高的安全强度。

从安全属性的观点可将攻击类型分成阻断攻击、截取攻击、篡改攻击、伪造攻击 4 类。从攻击方式可将攻击类型分为被动攻击和主动攻击两类。还可从攻击目的和效果将攻击类型分为访问攻击、篡改攻击、拒绝服务攻击、否认攻击。

风险是构成安全基础的基本观念,风险是丢失需要保护的资产的可能性。如果没有风险,就不需要安全。威胁是可能破坏信息系统环境安全的行动或事件,威胁包含目标、代理、事件 3 个组成部分。漏洞是攻击的可能的途径。风险是威胁和漏洞的综合结果。没有漏洞的威胁没有风险,没有威胁的漏洞也没有风险。

识别风险除了识别漏洞和威胁外,还应考虑已有的对策和预防措施。识别漏洞应寻找系统和信息的所有入口及分析如何通过这些入口访问系统。识别威胁是对目标、代理、动机及事件的识别。一旦对漏洞、威胁、预防措施进行了识别,就可确定对该组织的风险。

风险测量是确定由于攻击引起的代价,包括资金、时间、资源、信誉。对每个识别的风险判定风险测量的可能结果。综合这些信息,开发相应的风险管理项目。风险永远不可能完全去除,风险必须管理。

习　题

1. 对攻击可能性的分析在很大程度上带有(　)。

A. 客观性　　B. 主观性　　C. 盲目性　　D. 上面 3 项都不是

2. 网络安全最终是一个折中的方案,即安全强度和安全操作代价的折中,除增加安全设施投资外,还应考虑(　)。

A. 用户的方便性

B. 管理的复杂性

C. 对现有系统的影响及对不同平台的支持

D. 上面 3 项都是

3. 从安全属性对各种网络攻击进行分类,阻断攻击是针对(　)的攻击。

A. 机密性　　B. 可用性　　C. 完整性　　D. 真实性

4. 从安全属性对各种网络攻击进行分类，截获攻击是针对(　　)的攻击。

A. 机密性　　B. 可用性　　C. 完整性　　D. 真实性

5. 从攻击方式区分攻击类型，可分为被动攻击和主动攻击，被动攻击难以(　　)，然而(　　)这些攻击是可行的；主动攻击难以(　　)，然而(　　)这些攻击是可行的。

A. 阻止，检测，阻止，检测　　B. 检测，阻止，检测，阻止

C. 检测，阻止，阻止，检测　　D. 上面 3 项都不是

6. 窃听是一种(　　)攻击，攻击者(　　)将自己的系统插入到发送站和接收站之间。截获是一种(　　)攻击，攻击者(　　)将自己的系统插入到发送站和接收站之间。

A. 被动，无须，主动，必须　　B. 主动，必须，被动，无须

C. 主动，无须，被动，必须　　D. 被动，必须，主动，无须

7. 威胁是一个可能破坏信息系统环境安全的动作或事件，威胁包括(　　)。

A. 目标　　B. 代理　　C. 事件　　D. 上面 3 项都是

8. 对目标的攻击威胁通常通过代理实现，而代理需要的特性包括(　　)。

A. 访问目标的能力　　B. 对目标发出威胁的动机

C. 有关目标的知识　　D. 上面 3 项都是

9. 拒绝服务攻击的后果是(　　)。

A. 信息不可用　　B. 应用程序不可用

C. 系统宕机　　D. 阻止通信

E. 上面几项都是

10. 风险是丢失需要保护的(　　)的可能性，风险是(　　)和(　　)的综合结果。

A. 资产，攻击目标，威胁事件　　B. 设备，威胁，漏洞

C. 资产，威胁，漏洞　　D. 上面 3 项都不对

第3章 安全策略

本章要点：

- 安全策略的功能；
- 与网络安全有关的策略类型及其功能；
- 与网络安全有关的各种管理程序功能；
- 安全策略的生成、展开和有效使用。

3.1 安全策略的功能

安全策略对一个组织来说是十分重要的，是一个组织的信息安全部门能做的最重要的工作之一。它只涉及很少的技术知识，因而很多有专业技能的人似乎对其并不太重视，事实上，安全策略对他们也是非常重要的。

安全策略提供一系列规则，管理和控制系统如何配置，组织的员工应如何在正常的环境下行动，而当发生环境不正常时，应如何反应。安全策略执行两个主要任务。

1. 确定安全的实施

安全策略确定实施什么样的安全，具体内容如下：

(1) 安全策略确定恰当的计算机系统和网络的配置及物理安全的措施，以及确定所使用的合理机制以保护信息和系统。

(2) 安全策略不仅确定安全的技术方面，还规定员工应该执行某些和安全相关的责任(例如用户管理)，以及员工在使用计算机系统时所要求的行为。

(3) 安全策略还规定当非期望的事情发生时，组织应如何反应。当一个安全事故发生，或系统出故障时，组织的安全策略和安全程序规定其应做的事，以及在事故发生时，该组织的行动目标。

2 使员工的行动一致

对一个组织来说，确定实施什么样的安全是重要的，然而使每个工作人员行动一致以维护组织的安全也是同样重要的。安全策略为一个组织的员工规定一起工作的框架。组织的安全策略和安全过程规定了安全程序的目标和对象。将这些目标和对象告诉员工，就为安全工作组提供了基础。

3.2　安全策略的类型

一个组织内的安全策略和安全程序有很多种，本节将概述常用的、有效的安全策略和安全程序。在安全策略中，一般包含 3 个方面：

（1）目的

一个安全策略和安全程序应该有一个很好定义的目的，其文本应明确说明为什么要制定该策略和程序，及其对该组织有什么好处。

（2）范围

一个安全策略和安全程序应该有一个适用的范围。例如，一个安全策略可适用于所有计算机和网络系统，一个信息策略可适用于所有员工。

（3）责任

责任规定谁负责该文本的实施。不管谁负有责任，都必须经过很好的培训，明白文本的各项要求。

3.2.1　信息策略

信息策略定义一个组织内的敏感信息以及如何保护敏感信息。策略覆盖该组织内的全部敏感信息。每个员工有责任保护所有接触的敏感信息。

1. 识别敏感信息

根据该组织的业务，考虑哪些是敏感信息。敏感信息有可能包括经营业务记录、产品设计、专利信息、公司电话簿等。

某些信息对所有组织都是敏感信息，包括工资信息、员工家庭住址和电话号码、医疗保险信息、任何在公开以前的财务信息等。

值得指出的是，对一个组织来说，不是所有信息在所有时间都是敏感的。必须根据安全策略和安全程序很小心地确定什么是敏感信息。

2. 信息分类

对大部分组织而言，通常将信息分成二或三级已足够了，具体如下：

（1）最低级别的信息应该是公开的，也就是说，这些信息已为人所知，或能公开发表。

（2）再上一级的信息是不公开发表的，这些信息称为“私有”、“公司敏感”或“公司秘密”。这类信息对本组织员工是公开的，对某些组织外的人员需签不扩散协议才能得到。如果这些信息被公开或被竞争者得到，就有损于该组织。

（3）第三类信息称为“限制”或“保护”。这类信息被严格限制在一个组织内的很有限的员工范围内，不能向组织内的全体员工发布，更不能被组织外的人得到。

3. 敏感信息标记

对于非公开信息，安全策略应将各类敏感信息清楚地加上标记。如果以纸张的形式出现，应在每页的顶部和底部加标记，用字处理的页眉、页脚来实现。通常用醒目的大写

或斜体字标记。

4. 敏感信息存储

安全策略对存储在纸上或计算机系统中的敏感信息都应有相应的规定。

当信息存储在计算机系统中，安全策略规定相应的保护级别。可以是文件的访问控制，或对某些类型文件用合适的口令保护。极端情况需要加密措施。应该记住，系统管理员能看到计算机系统中的所有文本。如果该敏感信息不应被系统管理员知道，只有采取加密措施。

5. 敏感信息传输

信息策略必须确定如何传输敏感信息。可以用不同方法传输信息，如电子邮件、通过邮局邮寄、传真等。信息策略应对每种传输方法确定保护方法。

对通过电子邮件传送的敏感信息，安全策略应规定对用附件方式的文件或报文头进行加密。对硬拷贝信息的传送，需要签收收据的方式。对传真方式的传送，发送者需要用电话事先通知接收者等候在传真机旁。

6. 敏感信息销毁

留在纸上的敏感信息必须有相应的销毁方法。存储在计算机系统中的敏感信息，如果删除得不合适，仍有可能恢复。某些商业的软件工具已有更安全的方法，将敏感信息从介质中擦去。

3.2.2　系统和网络安全策略

安全策略规定计算机系统和网络设备安全的技术要求，规定系统或网络管理员应如何配置与安全相关的系统。这个配置也会影响用户。系统和网络管理员应对安全策略的实施负主要责任。

安全策略应定义每个系统实施时的要求，然而它不应规定对不同操作系统的专门配置，这属于专门配置的过程。

1. 用户身份及身份鉴别

安全策略应确定如何识别用户。通常安全策略应规定用于用户 ID 的标准或定义标准的系统管理过程。

更为重要的是，安全策略应确定对系统用户或管理员的基本的鉴别机制。如果机制是口令，则安全策略还应规定最小的口令字长、最长和最短的口令生存期以及口令内容的要求。

当开发安全策略时，每个组织还应决定是对管理员采用相同的机制，还是更强的机制。如果需要更强的机制，安全策略应确定相应的安全要求。更强的机制对诸如 VPN 或拨号访问这些远程访问也是适用的。

2. 访问控制

安全策略应确定对电子文件的访问控制的标准要求，具体如下：

(1) 在确定机制时，对计算机上的每个文件，用户定义的访问控制的某些方式应是可用的。这个机制应和身份鉴别机制一起工作，以确保只有授权用户能访问文件。该机制

至少应能确定什么样的用户有读、写、执行文件的许可。

(2) 对新文件的默认配置应说明当新文件生成时应如何建立许可。这部分安全策略应对给出的系统中的文件确定读、写、执行的许可。

3. 审计

安全策略的审计部分应确定所有系统上需要审计的事件类型。通常安全策略需对下列事件进行审计：成功或失败的登录、退出系统、对文件或系统的访问失败、成功或失败的远程访问、特权操作(由管理员操作,成功或失败)、系统事件(关机或重启)。

对每个事件应捕获下列信息：用户 ID、日期和时间、进程 ID、执行的动作、事件的成功或失败。

安全策略应说明审计记录应保存多久以及如何存放。如有可能,安全策略还应确定如何检查审计记录以及检查的时间间隔。

4. 网络连接

对每一种接到组织网络的连接形式,安全策略应说明连接的规则以及保护机制。

对拨号连接,应说明对这类连接技术的鉴别要求。该要求应指回到策略的身份鉴别这一部分。也可能描述一个比通常使用的更强的身份鉴别。

此外,安全策略应确定开始得到拨号访问的身份鉴别要求。对一个组织来说,应严格控制允许多少个拨号访问点,因此应公平地限制身份鉴别的要求。

一个组织的固定网络连接是由某些类型的固定通信线路接入的。安全策略应确定用于这些连接的安全设备类型。通常防火墙是合适的设备。仅仅说明设备类型并不意味着说明了相应的保护级别。安全策略应定义一个设备的基本网络访问控制策略以及请求和得到访问的过程。这些在标准的配置中是没有的。

对内部系统的远程访问是组织允许员工在外出时从外部访问内部系统。安全策略应说明这类访问所采用的机制。对这类访问,所有的通信应加密保护,并在加密部分说明密码类型。因为访问来自外部,应确定一个强的身份鉴别机制。

安全策略还应对允许员工得到这类访问的授权建立一个正确的过程。

5. 恶意代码

安全策略应确定搜索恶意代码(如病毒、特洛伊木马)的安全程序的存放位置。合适的位置包括文件服务器、桌面系统以及电子邮件服务器等。

安全策略应说明这些安全程序的要求,包括检查专门的文件系统的安全程序要求以及当这些文件打开时检查这些文件。策略还应要求对安全程序周期地更新签名。

6. 加密

安全策略应确定使用在组织内的可接受的加密算法,在信息策略中指出保护敏感信息的相应算法。安全策略不限制仅仅选择一种算法。安全策略还应说明密钥管理需要的过程。

3.2.3　计算机用户策略

计算机用户策略规定了谁可以使用计算机系统以及使用计算机系统的规则。

1. 计算机所有权

策略应清楚地说明所有计算机属于本组织，并且提供给员工在组织内用于工作相一致的用途。策略也可能禁止使用非组织的计算机用于组织的经营业务。例如，员工希望在家里做某些工作，组织将为其提供计算机，但只有组织提供的计算机可通过远程访问系统接到组织内部的计算机系统。

2. 信息所有权

策略应规定所有存储并用于组织内的计算机的信息属于组织所有。某些员工可能使用组织的计算机存储个人信息，如果策略没有特殊说明，则个人信息可分开存在私人目录下，并且非公开的。

3. 计算机的使用许可

大部分组织期望员工只使用组织提供的计算机，用于和工作有关的目的。但这不总是一个很好的假定。因此在策略中要明确说明，例如，组织的计算机只允许用于工作目的。

有时，组织允许员工为了其他目的使用组织的计算机，例如，允许员工晚上在内部网上玩游戏。如果是这样，应在策略中清楚说明。

使用组织提供的计算机还影响到什么软件加载到系统。规定非授权软件不允许装入系统。策略应规定谁可以装载授权软件以及怎样成为合法软件。

4. 没有隐私的要求

计算机用户策略中最重要的部分或许是规定在任何组织的计算机存储、读出、接收的信息都没有隐私。这对员工是十分重要的，他们应了解任何信息有可能被管理员检查，包括电子邮件。也就是说，使员工了解管理员或安全职员可能监视所有和计算机相关的动作，包括监视 Web 站点。

3.2.4　Internet 使用策略

Internet 使用策略经常包括在通用计算机使用策略中。然而，由于 Internet 的特殊性，有时将它作为单独的策略。Internet 的接入可以提高员工的工作效率。但 Internet 也给员工提供了一个滥用计算机资源的机会。

Internet 使用策略规定了如何合理地使用 Internet，诸如和业务有关的研究、采购，或使用电子邮件通信等；确定哪些是非正当使用，诸如访问和业务无关的 Web 站点、下载有版权的软件、音乐文件的交易、发送连锁邮件等。

假如该策略是从计算机用户策略分离出来的，它应说明组织有可能监视员工对 Internet 的使用，当员工使用 Internet 时，没有隐私的问题。

3.2.5　邮件策略

有些组织为电子邮件的使用开发了专门的策略。电子邮件正越来越多地用于组织的业务处理。电子邮件是使组织的敏感信息毫无价值的另一种方法。当一个组织选择定义

电子邮件策略时，应考虑到内外两方面的问题。

1. 内部邮件问题

电子邮件策略不应和其他的人力资源策略相冲突。例如，电子邮件策略应规定禁止利用电子邮件进行性骚扰；又如，规定在电子邮件中不用非正式用语和同伴通信。

如果组织要对电子邮件的某些关键字或附件进行监控，则策略应说明这类监控可能发生。策略还应对员工说明不能期望在电子邮件中有隐私。

2. 外部邮件问题

电子邮件可能包含一些敏感信息。邮件策略说明在什么条件下是可以接受的，并且在信息策略中指出该类信息应如何保护。也可能在外部邮件的底部指出相应的信息必须保护。

邮件策略还应识别进入的电子邮件问题。例如，很多组织测试进入的文件附件是否有病毒。该策略应指向组织的安全策略关于相应的病毒配置问题。

3.26　用户管理程序

用户管理程序是最容易被组织忽视的安全程序，因而提供了最大风险的可能。保护系统不被非授权者使用的安全机制是一个很好的事情，但是如计算机系统的使用没有合适的管理也将使其完全无用。

1. 新员工程序

应为新员工提供一个正确访问计算机资源的程序。应该由人力资源部门和系统管理员协同工作。理想的状况是新员工请求使用计算机资源，该新员工的管理者签发批准，然后系统管理员将为该新员工提供合适的系统和文件的访问。这个程序也应用于新的顾问和临时员工，并标明相应的有效期。

2. 工作调动的员工程序

对工作调动的员工也应开发一个专门的程序。这个程序的开发由人力资源和系统管理部门协作。员工原来的管理和新管理者应确定换到新岗位上的员工已经不需要原来的访问或者需要新的访问。相应的系统管理员依此进行变更。

3. 离职员工的程序

最重要的用户管理程序是将离职的员工从系统中除去。该程序也需人力资源和系统管理部门协作。当人力资源部认定一个员工离职，将提前通知相应的系统管理员，这样当该员工在职的最后一天就可将其账户停止。

3.27　系统管理程序

系统管理程序是确定安全和系统管理如何配合工作以使组织的系统安全。系统管理程序应确定各种和安全相关的系统管理如何完成。当谈及系统管理员监控网络的能力时，该程序应由计算机用户策略确定，并反映组织期望系统如何管理。

1. 软件更新

该程序应确定一个系统管理员多长时间检查新的补丁或从厂家升级。希望这些新的补丁不是当出现时刚刚安装,这样在补丁安装之前就规定测试。

最后,当这样的升级发生时(通常在维护窗口)该程序应做文档,当升级失败时放弃程序。

2. 漏洞扫描

每个组织应开发一个识别计算机系统漏洞的程序。通常由安全方面扫描漏洞,由系统管理做补丁。已有一些商业的和免费使用的扫描工具。

程序应确定多长间隔需进行扫描。扫描的结果应传给系统管理来纠错和执行。

3. 策略检查

组织的安全策略确定每个系统的安全要求。定期的外部或内部审计用来检查是否和策略一致。在审计时,安全应和系统管理一起工作以检查系统的一致。可以用自动的工具,也可以用手动进行。

4. 登录检查

来自各种系统的登录应定期检查。可以和安全员一起以自动方式检查这些登录。

如采用自动工具,程序应规定工具的配置以及希望它如何处理。如采用手动方式,程序应规定多长间隔检查登录文件以及事件类型等。

5. 常规监控

一个组织应该有一个程序归档说明何时网络通信监控发生。有些组织可能选择连续执行这种类型的监控,有些则选择随机监控。无论如何,总应进行监控,且归档。

3.2.8　事故响应程序

当计算机事故发生时,事故响应程序确定该组织将如何作出反应。根据事故的不同,事故响应程序应确定谁有权处理,以及应该做什么,但无须说明如何做。后者将留给处理事故的人决定。

1. 事故处理目标

当处理事故时,事故响应程序应确定该组织的目标,包括保护组织的系统、保护组织的信息、恢复运行、起诉肇事者、减少坏的宣传等。

这些目标不是唯一的,可以有多个目标。关键是要在事故发生前确定组织的目标。

2. 事件识别

识别一个事故或许是事故响应中最困难的一部分。某些事故是显而易见的,如 Web 站点的外貌被损坏。有些事故可能是由于入侵攻击或用户的误操作,如数据文件的丢失。

在公布事故以前,应由系统管理员做某些检查,以决定事故是否确实发生了。这部分程序能确定某些事件是显而易见的事故。而某些不是显而易见的事故,管理员应确定检查的步骤。

在得到决定事故的更多信息后，应组织一个事故响应组，应包括以下部门：安全、系统管理、法律、人力资源、公共关系等。

3. 信息控制

在发布事故消息时，组织要控制应发布什么样的信息。有多少信息需发布取决于该事故对组织及其客户的影响程度。信息发布的方式、方法也应考虑对组织的正面效应。

4. 响应

一个组织对事故流的响应直接取决于事故响应程序的目标。例如，保护系统和信息是目标，那么将系统从网络中移走，并进行必要的修复。另一种情况可能是保持系统在网上的在线状态以及继续服务或允许入侵者再回来，这样可对入侵者跟踪并设置陷阱。

5. 授权

事故响应的一个重要部分是决定事故响应组的负责人，授权采取行动，包括确定系统是否要离线，以及和客户、新闻机构、律师部门联系等。通常选择一个组织的官员来担任，在事故响应程序开发时就要确定负责人，而不是事故发生时决定。

6. 文档

事故响应程序应该规定事故响应组建立其行动档案。有两个好处，其一是有助于事故过后了解所发生的事件全过程；其二是如果要起诉，则有助于法律实施，对事故响应组也可作为一本参考手册，有助于他们处理事故。

7. 程序的测试

事故响应是很实际的，不能期望第一次使用事故响应程序，每一件事都很完美。因此，当开发完事故响应程序后，应广泛征求意见，找出其不足之处并改进。

事故响应程序还需在现实世界中测试，可以做一些模拟攻击，并观察其响应效果。这些测试可事先公布，也可不公布。

3.2.9　配置管理程序

配置管理程序规定修改组织的计算机系统状态的步骤。该程序的目的是确定合适的变化不会对安全事故的识别产生不好的影响。因此，新的配置要从安全的角度予以检查。

1. 系统的初始状态

对于一个新的系统，它的状态应有文档，包括操作系统及其版本、补丁水平、应用程序及其版本。

2. 变更的控制程序

当系统变更时，应执行配置控制程序。该程序应在变更实施前对计划的变更进行测试。当提出变更请求时，应将变更前后的程序存档。在变更以后，应更新系统配置以反映系统的新的状态。

3.2.10　设计方法

对生成新系统或能力的项目应有一个设计方法，以提供该组织生成新的系统的步骤。在设计之初就要考虑和安全有关的问题，使最后完成的系统能和安全策略相一致。设计过程中，与安全相关的步骤如下：

（1）需求定义

在任何一个项目的需求定义阶段，应将安全需求列入。设计方法应指出组织的安全策略和信息策略的要求。特别是要确定敏感信息和关键信息的要求。

（2）设计

在项目的设计阶段，设计方法应确保项目是安全的。安全人员应成为设计组成员或作为项目设计审查人员。在设计中对不能满足安全要求之处应特别指出，并予以妥善解决。

（3）测试

当项目进入测试阶段，应同时进行安全测试。安全人员应协助编写测试计划。安全要求有可能难以测试，例如，难以测试以确定入侵者不可能看到敏感信息。

（4）实施

项目实施阶段同样有安全要求。实施组应使用合适的配置管理程序。在新系统成为产品以前，安全人员应检查系统的漏洞和合适的安全策略规则。

3.2.11　灾难恢复计划

每个组织都应有一个灾难恢复计划。然而，很多组织却没有，因为他们认为灾难恢复计划要花很多钱，需要建立一个热备站，配置场地和必要的设备，以便随时接替运行。事实上，灾难恢复计划并不一定需要这样的热备站，可以是很简单的一些措施。只有当很多甚至全部计算机系统不可用，要决定该组织如何继续运行时，才会比较复杂。

一个恰当的灾难恢复计划应考虑各种故障的级别：单个系统、数据中心、整个系统。

1. 单个系统或设备故障

单个系统或设备故障包括盘、主板、网络接口卡、元件的故障。作为灾难恢复计划的一部分，应该检查组织的环境以识别任何单个系统或设备故障的影响。对每个故障，应在可允许的时间内修复并恢复运行。“可允许的时间”是根据对系统的关键程度以及解决方案所花的费用而定。

不论什么样的解决方案，灾难恢复计划必须能修复故障，使系统继续运行。灾难恢复计划必须和组织的运行部门结合，使他们知道应采取什么步骤恢复系统运行。

2 数据中心事件

灾难恢复计划还为数据中心的主要事件提供一个程序。例如，发生火灾，数据中心不能使用，应采取什么步骤重新恢复其能力。其中必须解决的一个问题是有可能丢失设备，灾难恢复计划应包括如何得到备用的设备。

假如数据中心不能用了，但仍有一些设备完好，灾难恢复计划应考虑如何添加新的设

备以及如何重建通信线路。热备站是一种解决方案，但费钱。如果没有热备站，灾难恢复计划应确定其他可能的场地，重新建造计算机系统。

3. 场地破坏事件

场地破坏事件是灾难恢复计划通常需要考虑的一类事件。虽然这类事件发生的概率较小，但对一个组织的危害极大。对每类事件，组织的每个部门都应参与。第一步是识别必须重建的关键能力，以使该组织继续生存。如果是一个电子商务站点，则最关键的系统可能是计算机系统和网络。如果是生产产品的工厂，则制造部门是关键，它的优先度高于计算机系统。

4. 灾难恢复计划的测试

灾难恢复计划是一个十分复杂的文档，通常不是一次写成就立即成功，因此需要测试。测试的必要性不仅在于检验其正确性，而且在于检查其是否处于备用状态。

灾难恢复计划的测试可能十分昂贵且有破坏作用。所以一个组织通常指定一些关键员工定期地对灾难恢复计划进行巡视，而且每年进行一次全面的测试。

3.3　安全策略的生成、部署和有效使用

3.3.1　安全策略的生成

安全策略的生成分成以下几步。

1. 确定重要的策略

对一个组织而言，并非需要所有有关安全的策略，而应确定哪些安全策略对该组织是重要的。这取决于该组织的业务性质，例如，一个组织需要通过 Internet 来传递信息，则灾难恢复计划比计算机使用策略更重要。

安全人员应该识别什么是最重要的安全策略，并与系统管理员、人力资源部门、咨询办公室协作，以确定哪些策略是最重要的。

2. 确定可接受的行为

某些员工的行为是可接受的，某些却是不可接受的，这取决于该组织的文化。例如，某些组织允许所有员工在 Internet 上冲浪，而没有任何限制。组织的文化使员工及管理者相信这样做能很好完成他们的任务。而另一个组织却对员工访问 Internet 有严格的限制，甚至限制从某些不可接受的 Web 站点下载软件。

这两个组织的策略完全不同。事实上，第一个组织决定根本无须实施 Internet 使用策略。对安全专业人员来说应该知道不是所有策略对所有组织都是适用的。安全专业人员在为一个组织草拟安全策略以前应花一些时间去了解该组织的文化以及员工的期望。

3. 征求建议

闭门生成安全策略是很少能成功的。安全专业人员在制定策略时应寻求组织的其他

部门的帮助。应该征求组织的总顾问以及人力资源部门的建议，此外，系统管理员、计算机系统用户以及物理安全部门的建议也是重要的。

一般来讲，凡是与实施策略有影响的人都应参与策略的制定过程，这样他们将了解什么是所期望的。

4. 策略的开发

首先拟出一个好的纲要，可以参考一些手册，如 RFC 2196 场地安全手册提供了各种策略的纲要。

根据纲要逐节草拟策略文档。在草拟过程中，还要不断听取上述有关人员的意见和建议。

在策略文档完成后，提交管理部门批准和实施。

3.3.2　安全策略的部署

安全策略的生成相对来说较容易，因为只需组织少部分人介入。但要有效地部署和实施，需要全体人员介入。

1. 贯彻

安全策略对每个部门都有影响，必须在各部门贯彻。由于在策略生成时，已征得各部门管理者的意见。这些管理者的介入大大有助于安全策略在各个部门的贯彻。这远比最高层领导强调安全策略的重要性、强调应予以贯彻更有效。

2. 培训教育

因为安全策略对组织的全体员工都有影响，所以安全专业人员必须负责对员工进行安全教育，人力资源部门和培训部门要协助进行。特别重要的是，当某些安全策略改变时会影响到全体员工，例如，如需更改口令，必须事先告知全体员工，否则会造成一时混乱。有时这种更改采用平滑过渡的方法更合适。

3. 执行

有时安全环境的突然改变会产生相反的效果，所以采取很好的计划和平滑过渡会更好。安全工作要与系统管理部门和其他有影响的部门密切配合，使执行更有效。

3.3.3　安全策略的有效使用

1. 新的系统及项目

一个新的系统及项目启动时，就应同时进行安全策略的程序设计。也就是说，将安全作为新系统和项目的设计的组成部分，使得安全要求在设计之初就能被识别和实施。

如果新系统不能满足安全要求，该组织就要知道存在的风险，并提供某些机制来管理存在的风险。

2. 已有的系统及项目

当一个新的安全策略被批准后，应该检查每个已有的系统，看其是否和新的安全策略相符合。如果不符合，确定是否可采取措施来遵守新的策略。应该和系统管理员以及使

用该系统的部门一起工作，使安全作相应的变更。这可能需要做一些开发工作，不能立即改变，会有一定的延迟。应在经费和系统设计限制条件下，和系统管理员及有关部门密切配合，及时地完成变更。

3. 审计

很多组织内部的审计部门，定期地审计系统看其是否遵守安全策略。安全部门应及时将新的安全策略通知给审计部门，并配合他们工作，使他们在审计时了解这些变更。一般来说，这个变更应是双向的。安全部门应向审计部门解释安全策略如何开发以及期望达到什么样的目标；审计部门应向安全部门解释审计如何进行以及审计的目标。他们之间应有某种约定，一种类型的系统应考虑相应类型的安全策略。

4. 安全策略的审查

即使是一个好的安全策略也不是一劳永逸的。应定期对每个策略进行审查，看其是否仍然适合于该组织。应对大部分策略每年审查一次。对某些程序，如事故响应程序或灾难恢复计划，可能需要更加频繁的审查。

在审查时，应和所有和安全有关的部门接触，听取他们对现有的安全策略的意见和建议。对重要的问题还可召开专门的调研会。在此基础上调整安全策略、申报批准、开始培训、贯彻实施。

3.4　本章小结

网络安全策略执行两个主要任务，其一是确定在一个组织内实施什么样的安全；其二是让组织内的员工行动一致，懂得需要什么样的安全。

信息策略定义一个组织内的敏感信息以及如何保护敏感信息。包括敏感信息识别、信息分类、敏感信息标记、敏感信息存储、敏感信息传输以及敏感信息销毁。

系统和网络安全策略规定计算机系统和网络设备安全的技术要求，规定系统或网络管理员应如何配置和安全相关的系统。系统和网络管理员应对安全策略的实施负主要责任。安全策略应包括用户身份及身份鉴别、访问控制、审计、网络连接、恶意码防止、加密等。

计算机用户策略规定了谁可以使用计算机系统以及使用计算机系统的规则。包括计算机所有权、信息所有权、计算机使用许可以及没有隐私的要求。

Internet 使用策略规定了如何合理地使用 Internet，确定哪些是 Internet 的非正当使用。

为了切实执行各种安全策略，还需开发各种管理程序，包括用户管理程序、系统管理程序、事故响应程序、配置管理程序、设计方法，以及灾难恢复计划。

要生成安全策略，需要确定什么是重要的策略，什么是员工可接受的行为，经过调研最后完成。安全策略的部署需要全体员工介入，通过宣讲、培训直到执行。安全策略的有

效使用需要将安全策略和系统设计同步进行，还需要定期审计和审查。

习　　题

1. 什么是网络安全策略执行的主要任务？
2. 网络安全策略应包含哪些内容？
3. 什么是信息策略的目的和内容？
4. 什么是计算机系统和网络安全策略的目的和内容？
5. 什么是计算机用户策略的目的和内容？
6. 什么是 Internet 使用策略的目的和内容？
7. 什么是系统管理程序的作用和内容？
8. 什么是事故响应程序的作用和内容？
9. 什么是灾难恢复计划的必要性及其内容？
10. 如何生成、部署和有效使用网络安全策略？

第4章 网络信息安全服务

本章要点：

- 针对不同攻击需要的基本安全服务；
- 机密性服务的类型及相应的机制；
- 完整性服务的类型及相应的机制；
- 可用性服务的类型；
- 可审性服务的基本功能；
- 身份鉴别的方法以及在网络环境下的身份鉴别；
- 数字签名原理；
- Kerberos 鉴别工作原理；
- 公钥基础设施结构；
- 访问控制基本原理。

为了维护信息自身的安全就要抵抗对信息的安全威胁。本章讲述用以对抗攻击的4个基本安全服务：机密性服务、完整性服务、可用性服务以及可审性服务。表4-1列出了针对不同攻击需要的安全服务。

表4-1　针对不同攻击需要的安全服务

安全服务 / 攻　击	机密性	完整性	可用性	可审性
访问攻击	×			×
篡改攻击		×		×
拒绝服务			×	
否　　认		×		×

用于一个组织内的特定的信息安全服务取决于相应的风险评估及安全计划。然而，清楚地知道一个组织的基本安全需求，对于更好地了解如何针对专门类型的攻击实施安全服务是很重要的。

4.1 机密性服务

机密性服务提供信息的保密。正确地使用该服务，就可防止非授权用户访问信息。为了正确地实施该服务，机密性服务必须和可审性服务配合工作，后者用来标识各个访问

者的身份，实施该功能，机密性服务能对抗访问攻击。机密性服务应考虑信息所在的形式和状态，比如，是物理形式的纸面文件、电子形式的电子文件，还是在传输中的文件。

4.1.1　文件机密性

文件的存在形式不同，文件的机密性服务的方式也相应不同。

对纸面文件，主要是存放这类文件的物理位置必须是可控的，通过物理位置的访问控制来保护文件的机密性。

对电子文件，有几种情况。首先文件可能同时存放在不同位置，如后备磁带、多个计算机系统、软盘或 CD 等。其次对电子文件的保护有些也需要物理位置的访问控制，如同保护纸面文件一样，例如，对磁带、磁盘需要物理访问控制。对于存放在计算机系统中的电子文件，则需要某些类型的计算机访问控制，也可能包括文件的加密。计算机访问控制要依靠合适的身份标识和身份鉴别(一种可审性服务)以及正确的系统配置，这样可防止非授权用户旁路身份标识和身份鉴别功能而成为合法用户。

为实现文件机密性服务，所需提供的机制包括物理安全机制、计算机文件访问控制以及文件加密。文件机密性的要求包括身份标识和身份鉴别、正确的计算机系统配置，如使用加密则还需合适的密钥管理。

4.1.2　信息传输机密性

仅仅保护存储在文件中的信息是远远不够的。信息有可能在传输过程中受到攻击，因此必须同时保护在传输中的信息机密性，图 4-1 表示使用加密来完成信息传输的机密性。

可基于每个报文信息进行加密保护，也可以对链路上的所有通信进行加密。加密能阻止窃听，但不能完全阻止信息的截获。为了防止信息被截获，需要合适的身份标识和身份鉴别，它可决定远程端点的身份，如图 4-2 所示。

4.1.3　通信流机密性

不同于上面所述的机密性服务，通信流的机密性并不关心正在传输或存储的信息本身的内容。它主要关心两个端点之间所发生的通信形式。这些信息形式通过通信分析可识别组织之间的通信情况。例如，很多新闻机构发现某一时刻有大量的快餐送至政府某重要机关，则可推测某些紧急事件甚至是危机可能发生。

在大量通信流的两个端点之间加入模糊(遮掩)信息流可提供通信流机密性服务。例如，在军队中，不论何时需要传送多少报文，都应设法使两个场地之间的通信流始终保护不变。这是可以做到的，当实际通信流小的时候，可以人为地加入填充通信。这样实际的通信流变化就无法被测定。

上面分析的 3 种机密性都可阻止访问攻击，然而仅仅依靠机密性服务并不能完全解决问题。机密性服务必须与可审性服务一起对企图访问信息的每个成员建立身份标识，两种服务结合起来可减少非授权访问的风险。

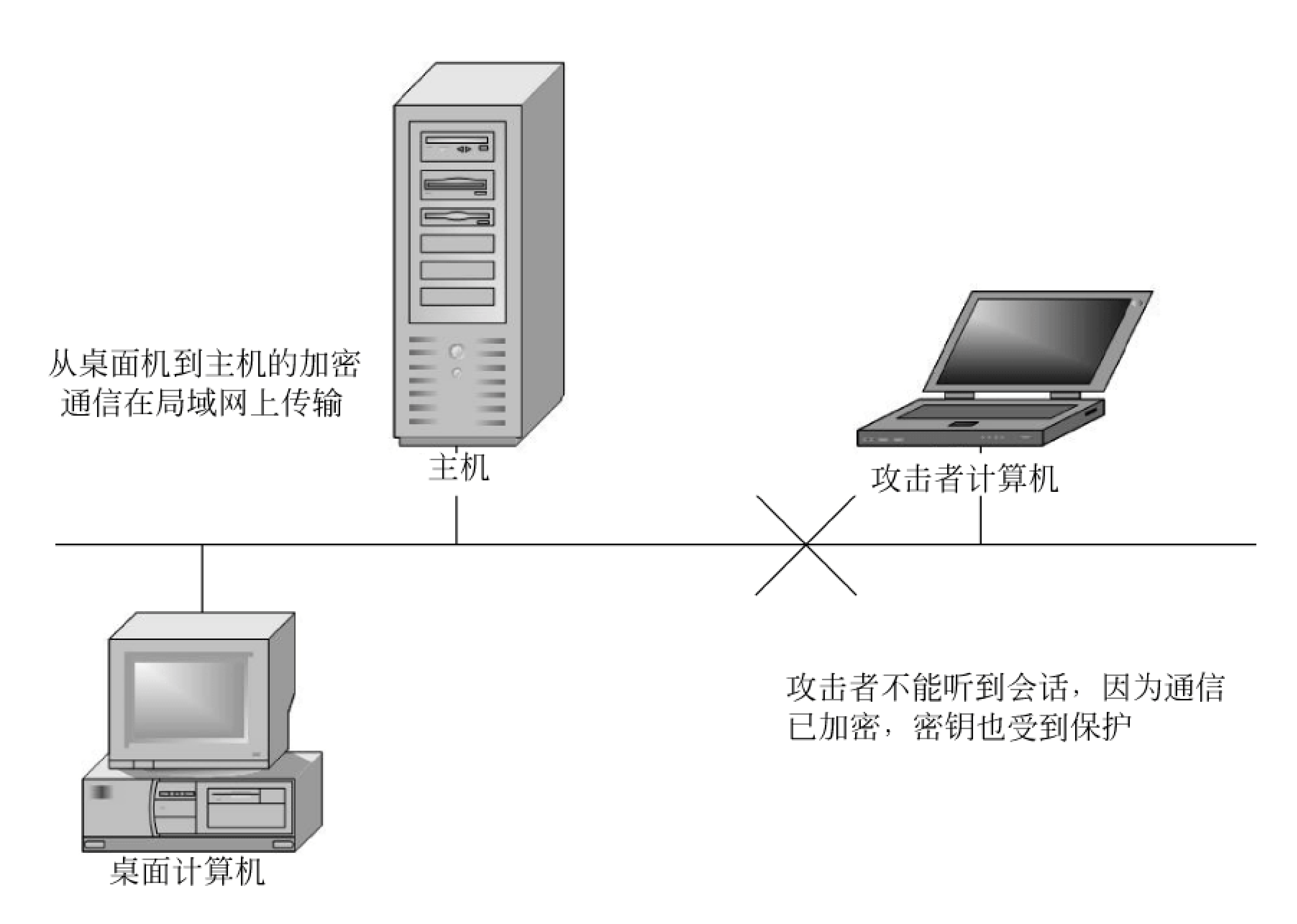


图 4-1　使用加密保护传输中的信息

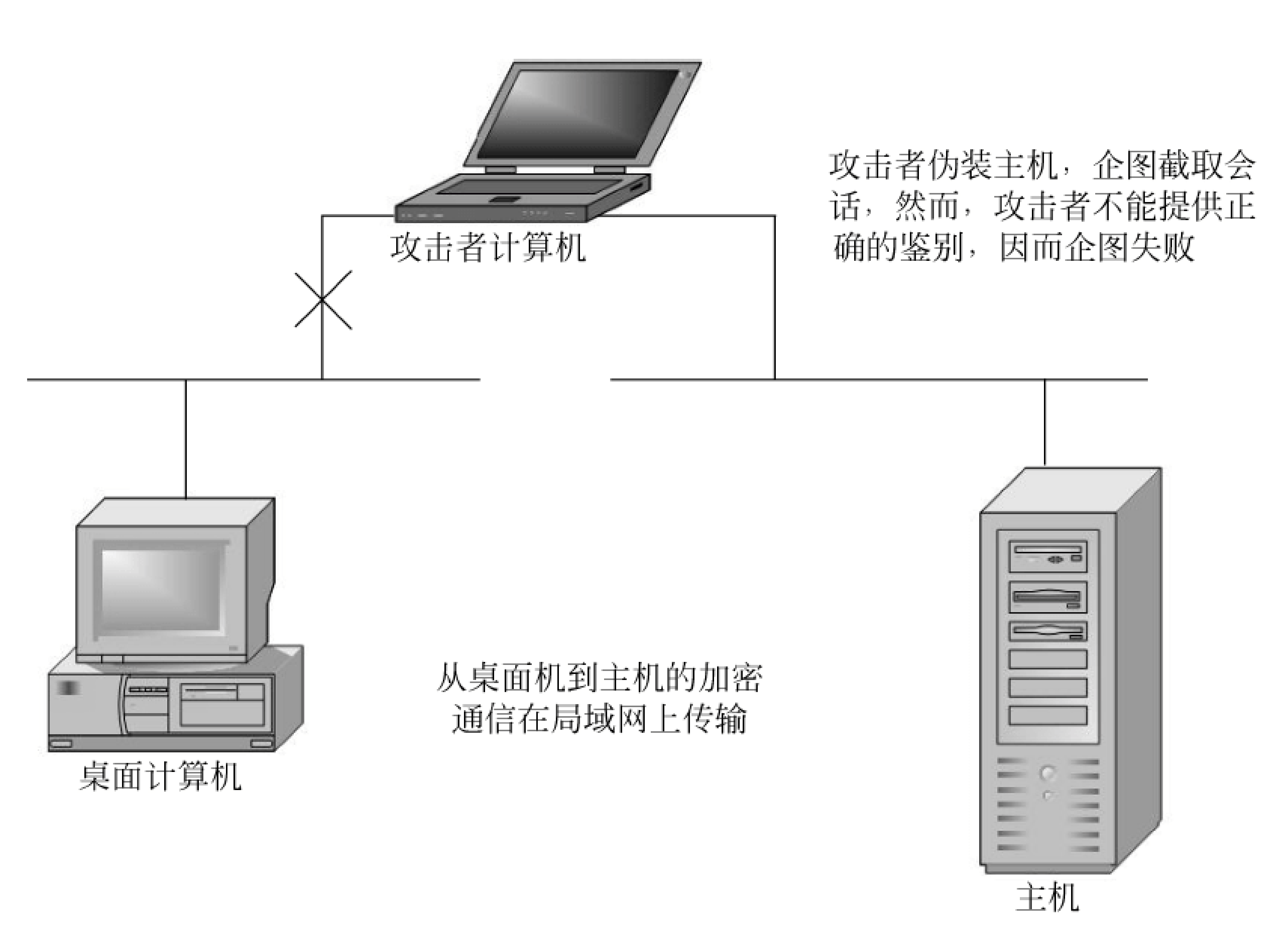


图 4-2　加密和身份标识、身份鉴别的结合

4.2　完整性服务

完整性服务提供信息的正确性。正确地使用完整性服务，就可使用户确信信息是正确的，未经非授权者修改过。如同机密性服务一样，该服务必须和可审性服务配合工作。

完整性服务能对抗篡改攻击。完整性服务同样应考虑信息所在的形式和状态。

4.2.1 文件完整性

文件的存在形式不同,文件的完整性服务方式也相应不同。一般来说,纸面文件的完整性较易识别,而纸面文件的修改要通过检查,修改者需要掌握一定技巧。而对于电子文件只要能访问它,任何人都能方便地对其进行修改。

为了防止修改纸面文件,可采用多种方法,包括在每一页上签名、装订成册、分发多个文件复制本等。这些完整性机制使修改变得十分困难,因为仿造签名技术、增加或删除装订成册的文件以及对一个文件的多个复制本同时进行修改都有很大难度。另一种方法是使用与机密性服务相同的机制,完全阻止非授权者访问文件。

对电子文件进行修改比较容易,使用字处理工具进行。保护电子信息完整性的最基本的方法是采用与保护信息机密性一样的方法,即计算机文件访问控制。然而不同的是,并不要求将访问控制机制配置成完全拒绝访问,而只需配置成只允许读文件,不允许写文件。如同机密性服务,十分重要的是必须正确识别那些企图修改文件的访问者。这只有通过身份标识和身份鉴别来实现。

假如文件驻留在单个计算机系统或者组织控制的网络中,对其进行计算机文件访问控制能达到很好的效果。如果需要将文件复制到其他部门或单位,那么只在单个计算机或可控网络上进行计算机文件访问控制就不足以提供充分的保护。因此需要有一种机制来识别非授权者对文件的改变。一种有效的机制就是数字签名,它必须与特定用户的识别一起工作。因此,完整性服务也必须和身份标识、身份鉴别功能结合在一起。

4.2.2 信息传输完整性

信息在传输中也可能被修改,然而如果不实施截获攻击就很难对传输中的信息进行修改。通常用加密方法可阻止大部分的篡改攻击。当加密和身份标识、身份鉴别功能结合在一起时,截获攻击便难以实现,如图 4-2 所示。

由上述分析可知,完整性服务可成功地阻止篡改攻击和否认攻击。任何篡改攻击都可能改变文件或传输中的信息,当完整性服务能检测到非授权者的访问,篡改攻击就不能成功进行。当完整性服务和身份标识、身份鉴别服务很好地结合,即使组织以外的文件被改变也能被检测出来。

如果没有好的完整性服务以及好的身份标识、身份鉴别服务,那么否认攻击也不可能被成功阻止。而检测这种攻击的机制是数字签名。

4.3 可用性服务

可用性服务提供的信息是可用的。可用性使合法用户能访问计算机系统,存取该系统上的信息,运行各种应用程序。可用性还提供两个计算机系统之间可用的传输信息的通信系统。当我们谈及信息和能力的可用性时,通常指的是电子信息。

4.3.1　后备

后备是最简单的可用性服务，是指对重要信息复制一份备份，并将其存储在安全的地方。后备可以是纸文件，如重要文本的备份；也可以是电子的，如计算机后备磁带。后备的作用是防止意外事件发生或文件被恶意破坏造成的信息完全丢失。

用于后备的安全位置可以是现场防火的地方，也可以是远地有物理安全措施的地方。

通常后备提供信息可用性，并不需要提供及时的后备。这意味着后备可能从远地检索到，然后传送到现场，并加载到相应的系统。

4.3.2　在线恢复

在线恢复提供信息和能力的重构。不同于后备，带有在线恢复配置的系统能检测出故障，并重建诸如处理、信息访问、通信等能力。它是通过使用冗余硬件自动处理的。

通常认为在线恢复是一种立即的重构，且无须进行配置。冗余系统也可以在现场备用，以便在原始系统发生故障时再投入使用。这种应用方式比大部分立即在线恢复系统更便宜。

4.3.3　灾难恢复

灾难恢复是针对大的灾难来保护系统、信息和能力。灾难恢复是当整个系统或重要的设备不可用时采取的重构一个组织的进程。

由上述分析可知，可用性是用来对拒绝服务攻击的系统恢复。可用性并不能阻止拒绝服务攻击，但可用性服务可用来减少这类攻击的影响，并使系统得以在线恢复、正常运行。

4.4　可审性服务

可审性服务本身并不能针对攻击提供保护，因此容易被人们疏忽。可审性服务必须和其他安全服务结合，从而使这些服务更加有效。可审性服务会增加系统的复杂性，降低系统的使用能力。然而，如果没有可审性服务，机密性服务与完整性服务也会失效。

4.4.1　身份标识与身份鉴别

身份标识与身份鉴别有两个目的：其一是对试图执行一个功能的每个人的身份进行标识；其二是验证这些人声称的身份。身份鉴别可使用以下任何一种或其组合的方法实现：

(1) 知识因子——你知道什么，如口令或 PIN(个人身份标识号)。

(2) 拥有因子——你有什么，如智能卡或标记。

(3) 生物因子——你是什么，如指印、视网膜。

组合使用上面的方法会更有效，如将口令和智能卡结合使用，通常称为双因子身份鉴

别。因为每一种身份鉴别方法本身有它自身的弱点，采用双因子鉴别可互相取长补短，因而更有效。例如，口令易于被猜测，而智能卡又易于被偷。生物因子身份鉴别难以伪造，但一定要将其指印放在指印扫描器中。

在物理世界，身份鉴别可以用带相片的 ID 卡出示给门警。指纹扫描器也经常用来对进入某些特定区域者作身份鉴别。这些身份鉴别机制将物理现场与每个人的身份标识直接联系起来。

在电子世界，物理身份鉴别机制并不适用。传统的用于计算机的身份鉴别机制是口令。身份标识是通过系统管理员设置的用户 ID 联系起来。系统管理员用某种方法来证明正在被鉴别的用户身份就是接收用户 ID 的个体。但是口令是单因子身份鉴别，有较大弱点。这就是为什么提倡在计算机系统中采用双因子身份鉴别，它提供更强的身份鉴别机制。

身份标识与身份鉴别也有助于计算机文件访问控制，以提供计算机系统电子文件的机密性和完整性。它对加密和数字签名也是重要的。然而，身份标识与身份鉴别必须要传给远程用户。远程用户要对本地机制证明它的身份标识。图 4-3 表示当发送一个报文时如何使用数字签名。用户首先对保护签名的本地机器作身份鉴别，然后本地机器允许使用签名机制，并发送已进行身份鉴别的报文。接收到该报文的用户使用数字签名以证明该报文的发送者的身份。

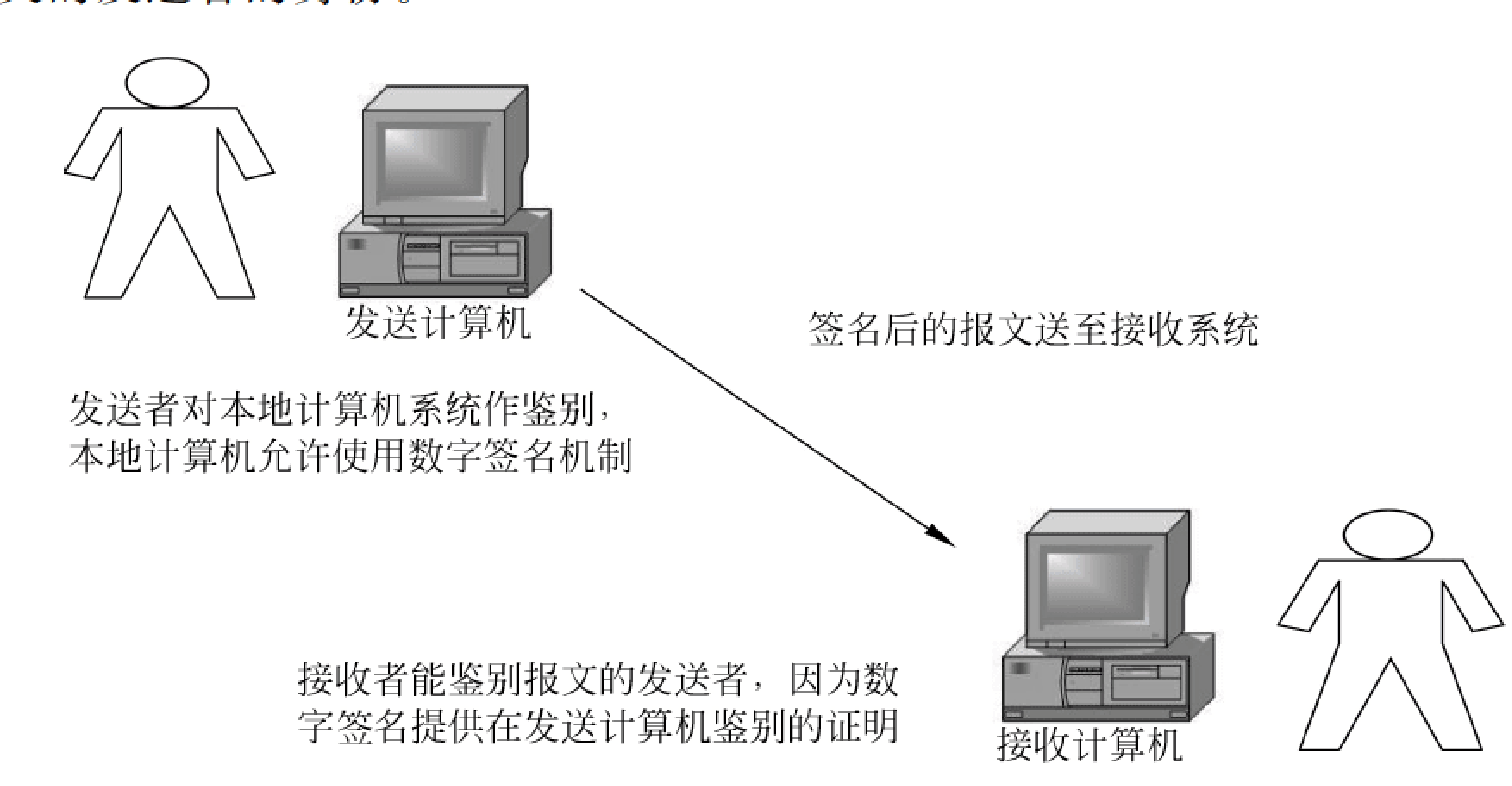


图 4-3　用于远程通信的身份标识与身份鉴别

在大多数情况下，身份标识与身份鉴别机制是一个组织内其他安全服务的关键。如果身份标识与身份鉴别失效了，那么完整性和机密性也无法保证。

4.4.2　网络环境下的身份鉴别

网络环境下的身份鉴别是验证某个通信参与方的身份是否与他所声称的身份一致的过程。一般通过某种复杂的身份认证协议来实现。身份认证协议是一种特殊的通信协议，它定义了参与认证服务的所有通信方在身份认证过程中需要交换的所有消息的格式、这些消息发生的次序以及消息的语义，通常采用密码学机制(例如加密算法)来保证消息的完整性、保密性。身份认证是建立安全通信的前提条件，只有通信双方相互确认对方身

份后才能通过加密等手段建立安全信道，同时它也是授权访问（基于身份的访问控制）和审计记录等服务的基础，因此，身份认证在网络安全中占据十分重要的位置。这些协议在解决分布式，尤其是开放环境，起着很重要的作用。其中系统的组成部分以及连接它们的网络可以跨越地理和组织的界限。

1. 身份认证技术

下面介绍两种身份认证技术。

(1) 口令技术

口令技术是常用的一种身份认证技术，使用口令存在的最大问题是口令的泄露。口令泄露可以有多种途径，例如，登录时被他人看见；攻击者从计算机中存放口令的文件中读到；口令被在线攻击猜测出；也可能被离线攻击搜索到。在线攻击是指在线状态下攻击者对用户口令进行的猜测攻击；离线攻击是指攻击者通过某些手段进行任意多数量的口令猜测，采用攻击字典和攻击程序，最终获得口令。离线攻击方法是 Internet 上常用的攻击手段。

(2) 采用物理形式的身份认证标记进行身份认证的鉴别技术

常用的身份认证标记是磁卡和智能卡。磁卡存储着关于用户身份的一些数据，用户通过读卡设备向联网的认证服务器提供口令才能证明自己的身份。最简单的智能卡称为 PIN(Personal Identification Number)保护记忆卡，PIN 是由数字组成的口令，只有读卡机将 PIN 输入智能卡后才能读出卡中保存的数据。这种卡比磁卡安全，可以存放一些秘密信息。另一种智能卡是加密挑战/响应卡，卡中有一个加密密钥，可使用该密钥进行加密和解密，但该密钥是无法被读出的。这种智能卡通常采用公开密钥算法，存储的是用户的私钥，可在离线状态下进行认证。在与计算机进行交互时首先递交代表自己身份的公钥证书，计算机验证证书的签发者后就获得了用户的公钥。

2 身份认证协议

基于密码学原理的密码身份认证协议比基于口令或者地址的认证更加安全，而且能够提供更多的安全服务。各种密码学算法，如私钥算法、公钥算法和哈希算法都可以用来构造身份认证协议，它们各有特点。可以分为共享密钥认证、公钥认证和零知识认证等几类。计算机可以存放高质量的密钥，进行复杂的加密解密运算。计算机可以代表用户进行加密解密操作，但是需要用户提供口令，将用户口令经过变换可以获得加密使用的密钥，或者是用口令来解密一个存放在某处的高质量的密钥，例如，用 PIN 获得存放 PIN 保护记忆卡中的高质量密钥。

身份认证协议一般有两个通信方，可能还会有一个双方都信任的第三方参与进行。其中一个通信方按照协议的规定向另一方或者第三方发出认证请求，对方按照协议的规定作出响应或者其他规定的动作，当协议顺利执行完毕时双方应该确信对方的身份。

(1) 会话密钥

在很多协议中，不仅要求验证相互身份，而且还要建立后续通信使用的会话密钥。会话密钥(Session Key)是指在一次会话过程中使用的密钥，一般都是由机器随机生成的。

会话密钥在实际使用时往往是在一定时间内都有效，并不真正限制在一次会话过程中。虽然公开密钥系统也被用于认证协议中，但是由于公钥系统算法复杂度高，大量数据的加密还是采用传统密码，因此会话密钥都是传统密钥。因为会话密钥主要用于通信加密，因此也将它称为通信密钥，与用于身份认证的认证密钥加以区分。会话密钥能够有效地抵抗密码分析攻击；而认证密钥不能长时间使用，否则容易被攻击者搜集到足够的密文数据进行密码分析。需要建立会话密钥的认证协议也被称为密钥分发协议。

（2）共享密钥认证

共享密钥认证的思想是从通过口令认证用户发展来的。传统方式是检验对方传递来的口令是否正确，但是这样口令容易在传递过程中被窃听而泄露。必须采用既能够验证对方拥有共同的秘密又不会在通信过程中泄露该秘密的方法，挑战/响应技术可完成这一目标。

在网络环境下，一台计算机可能要与很多台计算机进行身份认证，如果全部采用挑战/响应方式认证，那么就需要与众多的计算机都建立共享密钥。这样做在大型网络环境中既不经济也不安全，同时大量共享密钥的建立、维护和更新将是非常复杂的事情。

密钥分发中心（Key Distribution Center，KDC）的概念是 Needham 和 Schroeder 在 1978 年提出的，KDC 在网络环境中为大家所信任，并且与每个网络通信方都有一个共享密钥。网络中每个通信参与方都只与 KDC 有共享密钥，它们之间的认证需要借助于可信第三方 KDC 才能完成。KDC 负责给通信双方创建并分发共享密钥，通信双方获得共享密钥后再利用挑战/响应协议建立相互信任关系。

（3）公钥认证

公开密钥算法的出现为身份认证协议带来了更强有力的方法和手段，因为它可以让对方通过密码运算验证自己的身份而不需要将自己的私钥告诉对方。在公钥算法中，一般将利用私钥对明文信息进行的变换称为签名（sign），变换后的信息为签名信息；将利用公钥对明文信息进行的变换称为封装（seal）或者加密。

使用公钥方式进行身份认证时需要事先知道对方的公钥，虽然已经有算法可以解决双方在通信时直接交换公钥的安全问题，但是从使用方便程度和可管理程度上出发需要依靠一个可信第三方来参与分发公钥。如果没有可信第三方的参与，每个通信参与方都需要记住所有其他用户的公钥，不仅增加负担而且无法更新维护；其次每个通信方产生自己的私钥和公钥，而它们的可信赖程度不同，一旦出现问题和纠纷需要权威中间机构进行仲裁。在实际网络环境中，采用证书（certificate）的方式来分发公钥。证书是一种特殊格式的数据记录，它包含有证书代表的通信参与方的名字、身份信息、公钥以及签发机构、签发日期、序列号、有效期等相关数据，由证书权威机构（Certificate Authority，CA）用自己的私钥进行签名。证书权威机构扮演可信第三方的角色，它是大家信任的组织、机构。所有的公钥认证系统都采用了证书方式，证书被设计存放在目录服务系统中，通信参与方拥有 CA 的公钥，可以从目录服务中获得通信对方的证书，通过验证 CA 签名可以相信证书中列出的对方公钥。

KDC 方式和 CA 方式是分发密钥的主要技术，它们各有自己明显的优势和缺陷。公钥方式的身份认证协议安全强度要高，但是计算开销大，因此，越来越多的安全系统倾向

于利用公钥进行认证和建立对称的会话密钥，利用传统密钥进行大量数据传输的方法，例如，SSL 协议、PGP 等。

4.4.3　审计功能

可审性的另一个重要功能是审计。审计提供历史事件的记录。审计记录将每个人与其在计算机系统中或在物理世界中的行动联系起来。如果没有正确的身份标识与身份鉴别，审计记录也是没有用的，因为无法保证这些记录事件确实是谁执行的。

在物理世界，审计的方法有入门的日志、签名本、录像仪等。这些物理记录的目的是提供执行各种行动的记录。应该特别指出的是，必须采用完整性服务以保证这些审计记录没有被修改过。否则，这些审计记录是值得怀疑的。

在电子世界，计算机系统提供日志，以记录用户 ID 的行动。假如身份标识与身份鉴别功能的作用合适，这些事件就能跟踪用户的行为。同样，必须保护好计算机系统上的审计记录，防止非授权者对其进行修改，事实上，审计记录要防止任何人的修改。

由上述分析可知，可审性服务并不能阻止攻击。它与其他服务结合，尤其是机密性和完整性服务结合，对试图执行某些操作者进行正确的身份标识与身份鉴别。可审性服务还提供用户对系统执行的操作记录，因此，事件能重构。

4.5　数字签名

在完整性服务与可审性服务中都提到数字签名。数字签名是通信双方在网上交换信息用公钥密码防止伪造和欺骗的一种身份认证。在传统密码中，通信双方用的密钥是一样的，既然如此，收信方可以伪造、修改密文，发信方也可以抵赖他发过该密文，若产生纠纷，将无法裁决谁是谁非。

由于公钥密码的每个用户都有两个密钥，所以实际上有两个算法，如用户 A，一个是加密算法 E_A，一个是解密算法 D_A。

若 A 要向 B 送去信息 m，A 可用 A 的保密的解密算法 D_A对 m 进行加密得 $D_A(m)$，再用 B 的公开算法 E_B对 $D_A(m)$进行加密得

$$C=E_B(D_A(m))$$

B 收到密文 C 后先用他自己掌握的解密算法 D_B对 C 进行解密得

$$D_B(C)=D_B(E_B(D_A(m)))=D_A(m)$$

再用 A 的公开算法 E_A对 $D_A(m)$进行解密得

$$E_A(D_A(m))=m$$

从而得到了明文 m。

由于 C 只有 A 才能产生，B 无法伪造或修改 C，所以 A 也不能抵赖，这样就能达到签名的目的。不是所有公钥系统都具有数字签名的能力，RSA 第一个提出这样的功能。

4.6　Kerberos 鉴别

Kerberos 鉴别是一种使用对称密钥加密算法来实现通过可信第三方密钥分发中心(KDC)的身份认证系统。它是美国麻省理工学院(MIT)为了保护 Athena 项目中的网络服务和资源而开发的,Kerberos 版本 5 的协议已被 Internet 工程部 IEIF 正式接受为 RFC 1510。

Kerberos 在学术界和工业界都获得了广泛的支持,被众多系统选作身份认证的基础平台。例如,开放软件基金会(Open Soft Foundation,OSF)开发的分布式计算环境 DCE 就是以 Kerberos 为身份认证平台的,而在国外应用最广泛的分布式文件系统(Andrew File System,AFS)也采用了 Kerberos 作为身份认证平台。目前各主要操作系统都支持 Kerberos 认证系统,例如,Microsoft 公司在其高端服务器产品 Windows NT 5.0 中也支持 Kerberos 系统。Kerberos 实际上已经成为工业界的事实标准。

Kerberos 使用对称密钥加密算法来实现通过可信第三方密钥分发中心的认证服务,它提供了网络通信方之间相互的身份认证手段,而且并不依赖于主机操作系统和地址。Kerberos 设计的目标是在开放网络上运行,不要求网络上所有主机的物理安全,同时还假设通过网络传输的包可以被任意截获、修改和插入。Kerberos 系统非常适合在一个物理网络并不安全的环境下使用,它的安全性经过了实践的考验。

Kerberos 协议中有 3 个通信参与方：需要验证身份的通信双方及一个双方都信任的第三方,即密钥分发中心(KDC)。当某个网络应用进程需要访问另外一个服务进程时,例如,向远程 FTP 服务器发起 FTP 连接,它首先需要向 FTP 服务器验证自己的身份,同时也要确认该 FTP 服务器的身份,这样就构成了双向的身份认证。将发起认证服务的一方称为客户方,将客户方需要访问的对象称为服务器方。在 Kerberos 中客户方是通过向服务器方递交自己的“凭据”(ticket)来证明自己的身份的,该凭据是由 KDC 专门为客户方和服务器方在某一阶段内通信而生成的。凭据中包括有客户和服务器方的身份信息、在下一阶段双方使用的临时加密密钥(称为会话密钥,Session Key),还有证明客户方拥有会话密钥的身份认证者(authenticator)信息。身份认证者信息的作用是防止攻击者将来将同样的凭据再次使用。

凭据是 KDC 发出的。Kerberos 在 Needham-Schroeder 原始模型中加入了时间标记(timestamp)以检测重放攻击(Replay Attack)。与 KDC 共享的密钥构成了客户方或者服务器方相信它接收到的凭据的真实性的基础。为了提高安全性能,一个 Kerberos 凭据只在一段有限的时间内有效,称为凭据的生命期。当生命期过后凭据自动失效,以后的通信必须从 KDC 获得新的凭据进行认证。

KDC 自治管理的计算机和用户等通信参与方的全体称为领域(realm),领域是从管理角度提出的概念,与物理网络或者地理范围等无关。在实际使用中,为了方便,通常选择与 Internet 域名系统一致的名字来命名领域。不同领域中的用户之间的身份认证也是可以进行的,Kerberos 定义了通过共享密钥进行领域间用户认证的方式。

Kerberos 保持一个它的客户方以及密钥的数据库，这些密钥是 KDC 与客户方之间共享的，是不能被第三方知道的。如果客户是用户，该密钥就是用户口令经过 Hash 生成的，需要使用 Kerberos 认证服务的其他网络服务也需要进行登记并且在登记时协商共享密钥，这些密钥往往是机器随机生成的。

4.7　公钥基础设施

公钥基础设施(PKI)是在分布式计算机系统中提供的使用公钥密码系统和 X.509 证书安全服务的基础设施。PKI 产品和服务允许使用者在网络上建立一个安全领域，在该领域中可以签发密钥和证书。PKI 支持使用者在建立的安全领域中进行加密密钥和证书的使用和管理，提供密钥管理(包括密钥更新、恢复和托管)、证书管理(包括产生和撤销)，以及安全政策管理等。PKI 还提供通过证书层次结构(Certificate Hierarchy)或者通过直接交叉证书(Cross Certificate)的方法在本地安全领域与其他安全领域之间建立相互信任的关系。

图 4-4 表示了 PKI 的体系结构，除了证书以外，PKI 还包括其他几个组成成分。PKI 最基本的组成是证书的主体，它通常是用户，也可以是任何拥有公钥的一个公司、组织、系统或者应用。例如，Web 站点就可以成为证书主体，它通过 SSL 或者其他协议与浏览器建立安全通信信道。用户和应用软件系统可以成为证书的客体，它们和其他实体也将是证书的使用者。

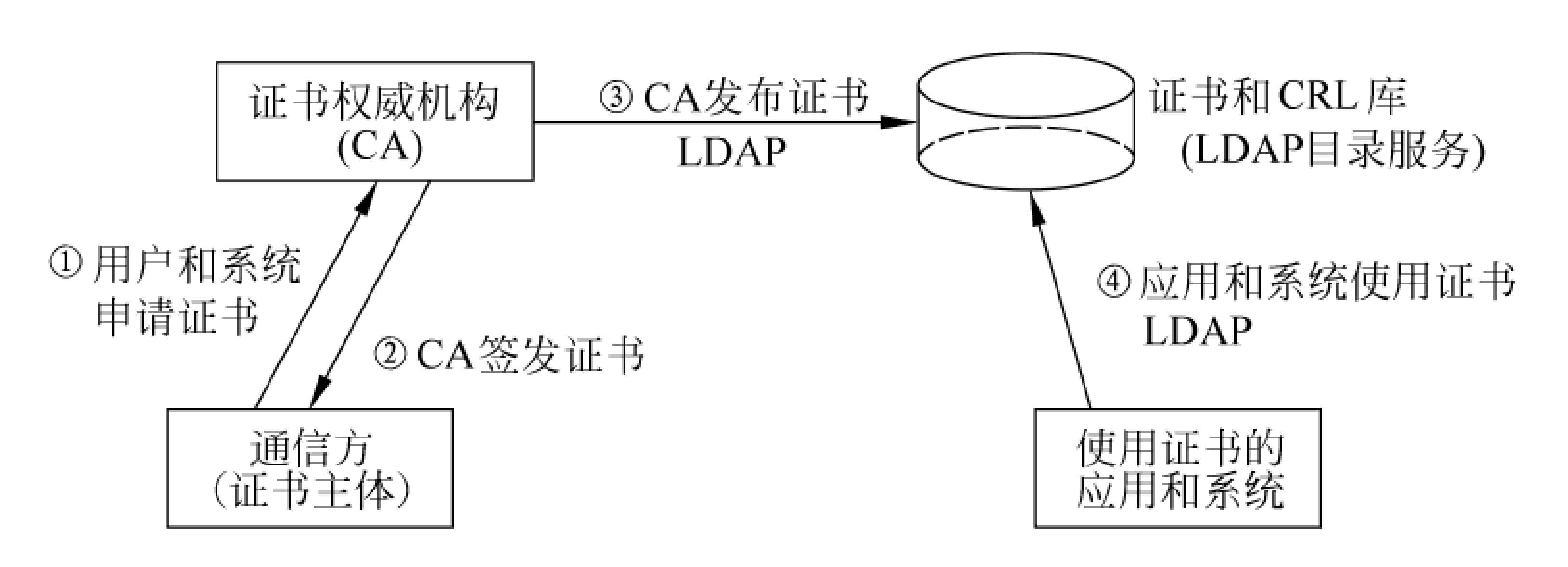


图 4-4　PKI 体系结构

证书权威机构(CA)创建并签发证书。通常一个 CA 将为一个有限的用户团体签发证书，这样的用户团体通常被称为安全领域(Security Domain)。CA 还维护并且发布证书撤销列表(Certificate Revoke List，CRL)，当证书以及证书中的公钥失效时通常采用 CRL 这种集中方式通知用户和应用。CA 通常将 CRL 发布在目录服务的某个位置甚至某个特定的 URL 上。

目录系统是 PKI 的重要依靠，目前支持轻量级目录服务(Light Weight Directory Access Protocol，LDAP)是最基本的要求。因为 PKI 将使用目录服务来存放、发布、查找和获取密钥，如果目录服务不支持基于证书的对象类和属性的话，PKI 产品通常将涉及对目录服务的扩展。由于 LDAP 和 X.509 是目前占优势的目录服务标准，大多数 PKI 产品

默认支持 X.509(X.520、X.521 和 X.509)定义的证书对象类和属性。

由于建立 PKI 的目标是需要与其他网络以及 Internet 互联,在全球范围内实现电子商务和安全通信等应用,因此,PKI 必须基于国际标准以保证它的互操作性,这是实现 PKI 的最低限度的要求。但是目前 PKI 体系结构和标准才刚刚推出,现有的很多证书服务器产品,例如,Netscape 的 Certificate Server 和 Microsoft 的 Certificate Server,只涉及了证书的生成和撤销,并没有解决密钥等其他问题,因此并不是一个完整的 PKI 的解决方案,没有完全解决企业对于公钥体系结构的需求。

4.8 访问控制

1. 访问控制概念

机密性服务和完整性服务都需要实施访问控制。访问控制是确定来访实体有否访问权以及实施访问权限的过程。被访问的数据,如文件、数据报文、分组数据包、数据帧等,统称客体。能访问或使用客体的活动实体称作主体,如用户以及作为用户代理的进程、作业或任务等。访问控制一般都是基于安全策略和安全模型的。Lampson 提出的访问矩阵(Access Matrix)是表示安全政策的最常用的访问控制安全模型。该矩阵中列表示访问者,即主体;行表示被访问对象,即客体。访问者对访问对象的权限就存放在矩阵中对应的交叉点上。

为节省存储空间,实际系统通常并不直接采用矩阵,而是采用访问控制表或者权利表进行表示。前一种方法是按照行来存储矩阵,在对象服务器上存储着每个对象的授权访问者及其权限的一张表,也称访问控制表(Access Control List,ACL)。负责保护访问对象的程序称为引用监控器(Reference Monitor),它根据访问控制表的内容来判断是否授权某个访问者某些访问权限。后一种方法则是按照列来处理矩阵,每个访问者存储有访问权利(capability)的表,该表包含了他能够访问的特定对象和操作权限。引用监视器根据验证访问表提供的权利表和访问者的身份来决定是否授予访问者相应的操作权限。

2 访问控制分类

根据能够控制的访问对象粒度可以将访问控制分为粗粒度(Coarse Grained)访问控制、中粒度(Medium Grained)访问控制和细粒度(Fine Grained)访问控制。这里并没有严格定义的区分标准,但是人们通常认为能够控制到文件甚至记录对象的访问控制可以称为细粒度访问控制,而只能控制到主机对象的访问控制称为粗粒度访问控制。

目前很多计算机系统的安全都是采用 ACL 模型,分布式系统和网络系统也不例外,ACL 模型提供安全保密和完整性安全策略的基础。

源通信参与方是通信发起者和请求者,请求信息包含了对网络资源进行某种操作的请求;ACL 服务器通过引用监控器检查源通信方的请求内容并决定是否允许通过;访问对象是网络资源,如文件、设备或者 CPU 等。

3. 访问控制实现

在集中式系统中访问控制是很容易实现的，因为操作系统控制着所有访问对象并且管理所有进程，所有操作均在主机操作系统管理下进行。在分布式系统和网络环境中情况有些不同，首先是访问者和被访问对象不在一台主机上，它们之间的通信路径可能很长并且中间可能经过很多台主机，这些主机的可信赖程度是不同的。因此，在进行身份认证时必须将远程用户和本地用户加以区分，在设置访问控制权限时也要区别对待。例如，有些资源只允许用户在本地进行访问。其次是规模不同，网络系统的规模比集中式系统要大很多，因此不可能由单个主机来负责管理所有用户以及他们的访问控制信息。必须有机制保证引用监视器与这些用户管理和访问控制信息管理的服务器之间安全地通信，这里涉及访问控制信息数据完整性和对访问控制服务器的认证协议等问题。

为了简化管理，访问者通常被分类成组、组织，设置访问控制时可以按组进行设定，这样就可以避免访问控制表过于庞大。例如，某文件允许所有清华大学学生阅读，那么在访问控制表中将清华大学学生作为组来定义是合适的，否则就需要在 ACL 中添加一万多项，而且随时需要根据学生毕业、入学而修改。当然，这需要身份认证系统提供分组管理的功能。

网络资源包括信息资源和服务资源。授权控制框架是对网络资源进行授权管理和访问控制的基本框架，它独立于各种应用系统，独立于各个安全子系统的授权管理系统，对网络资源实施统一管理，是网络资源管理的最主要的安全机制。授权控制框架可对各种应用服务进行授权管理，包括 WWW 应用、客户机/服务器应用、TCP/IP 应用、数据库应用、面向对象的分布系统应用 CORBA、报文队列 MQ 应用等标准应用对象。授权管理系统提供的基本服务是授权管理，管理和维护授权策略、对象映射、用户角色等，并且要有使用方便的管理界面，可以进行安全的远程管理。应用服务系统通过授权应用程序接口获取授权信息，实施用户对对象的访问控制。授权控制框架也应基于国际标准以保证它的互操作性。

4.9　本章小结

网络信息基本安全服务是为了维护信息自身的安全，针对信息安全威胁，用以对抗攻击的基本安全服务：机密性服务、完整性服务、可用性服务、可审性服务。

机密性服务提供信息的保密。机密性服务包括文件机密性、信息传输机密性以及通信流的机密性。相应的机制有访问控制、加密、填充通信等。机密性服务可阻止访问攻击，但它必须与可审性服务一起使用。

完整性服务提供信息的正确性。完整性服务包括文件完整性、信息传输完整性。相应的机制有访问控制、加密、数字签名等。完整性服务可成功地阻止篡改攻击和否认攻击，但它也必须与可审性服务一起使用。

可用性服务提供的信息是可用的，使合法用户能访问计算机系统、存取该系统上的信息、运行各种应用程序。可用性服务包括后备、在线恢复和灾难恢复。可用性服务是针对

拒绝服务攻击的一种安全服务。可用性并不能阻止 DoS 攻击，但可用来减少这类攻击的影响。

可审性服务包括身份标识与身份鉴别、审计。可审性服务本身并不能针对攻击提供保护，它必须和其他安全服务结合，从而使这些服务更有效。可审性服务会增加系统的复杂性，降低系统的使用能力。然而，如果没有可审性服务，机密性服务与完整性服务也会失效。

身份鉴别的方法有知识因子、拥有因子、生物因子以及它们的组合。网络环境下的身份鉴别是指可靠地验证某个通信参与方的身份是否与他声称的身份一致的过程，一般通过某种复杂的身份认证协议来实现。

数字签名是通信双方在网上交换信息用公钥密码防止伪造和欺骗的一种身份认证。

Kerberos 鉴别是一种使用对称密钥加密算法来实现通过第三方密钥分发中心(KDC)的身份认证系统。

公钥基础设施(PKI)是在分布式计算机系统中提供的使用公钥密码系统和 X.509 证书安全服务的基础设施。

访问控制是指确定可给予哪些主体访问的权利、确定以及实施访问权限的过程。被访问的数据统称客体，能访问或使用客体的活动实体称主体。访问控制一般都是基于安全政策和安全模型的。

习　　题

1. 机密性服务提供信息的保密，机密性服务包括(　)。
   A. 文件机密性　B. 信息传输机密性　C. 通信流的机密性　D. 以上 3 项都是

2. 完整性服务提供信息的正确性。该服务必须和(　)服务配合工作，才能对抗篡改攻击。
   A. 机密性　B. 可用性　C. 可审性　D. 以上 3 项都是

3. 数字签名要预先使用单向 Hash 函数进行处理的原因是(　)。
   A. 多一道加密工序使密文更难破译
   B. 提高密文的计算速度
   C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度
   D. 保证密文能正确地还原成明文

4. Kerberos 的设计目标不包括(　)。
   A. 认证　B. 授权　C. 记账　D. 加密

5. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别的叙述不正确的是(　)。
   A. 身份鉴别是授权控制的基础
   B. 身份鉴别一般不用提供双向的认证
   C. 目前一般采用基于对称密钥加密或公开密钥加密的方法
   D. 数字签名机制是实现身份鉴别的重要机制

6. 基于通信双方共同拥有的但是不为别人知道的秘密，利用计算机强大的计算能力，以该秘密作为加密和解密的密钥的认证是(　)。

A. 公钥认证　B. 零知识认证　C. 共享密钥认证　D. 口令认证

7. Kerberos 在请求访问应用服务器之前，必须(　)。

A. 向 Ticket Granting 服务器请求应用服务器 ticket

B. 向认证服务器发送要求获得“证书”的请求

C. 请求获得会话密钥

D. 直接与应用服务器协商会话密钥

8. 下面不属于 PKI(公钥基础设施)的组成部分的是(　)。

A. 证书主体　B. 使用证书的应用和系统

C. 证书权威机构　D. AS

9. 下列对访问控制影响不大的是(　)。

A. 主体身份　B. 客体身份

C. 访问类型　D. 主体与客体的类型

10. 为了简化管理，通常对访问者(　)，避免访问控制表过于庞大。

A. 分类组织成组

B. 严格限制数量

C. 按访问时间排序，并删除一些长期没有访问的用户

D. 不作任何限制

第5章 安全体系结构

本章要点:

- 可信系统体系结构及其要素;
- 网络安全的分层体系结构;
- OSI 安全体系结构的安全服务与安全机制;
- ISO/IEC 网络安全体系结构。

5.1 系统安全体系结构

5.1.1 可信系统体系结构概述

从头开始设计一个系统是一项复杂的任务,有很多复杂的、抽象的目标需要通过数学、逻辑、设计、编程、实施来达到。当构建一个系统时,需要做出很多基本的设计决定。安全仅仅是系统的一个目标,但这是需要十分重视的一个目标。

完整性、可用性、保密性可以在企业的不同地方实施。例如,一个公司可将客户的信用卡信息存储在数据库,很多用户可访问。很显然,这些信息需要很好地保护,以确保不被非授权用户访问或修改。先从一般性的问题开始,然后逐步细化。这些问题是:这些保护应放置在何处?当用户登录和授权时应否设置访问控制以指明什么数据能访问或不能访问?存储信用卡信息的数据文件是否应在文件一级予以保护?是否应提供限制用户的操作和活动的保护?是否需要将上述保护组合在一起?首先,也是最重要的问题是何处应设置保护,是在用户端,是在存储数据的地方,还是限制用户的活动?如图5-1所示。

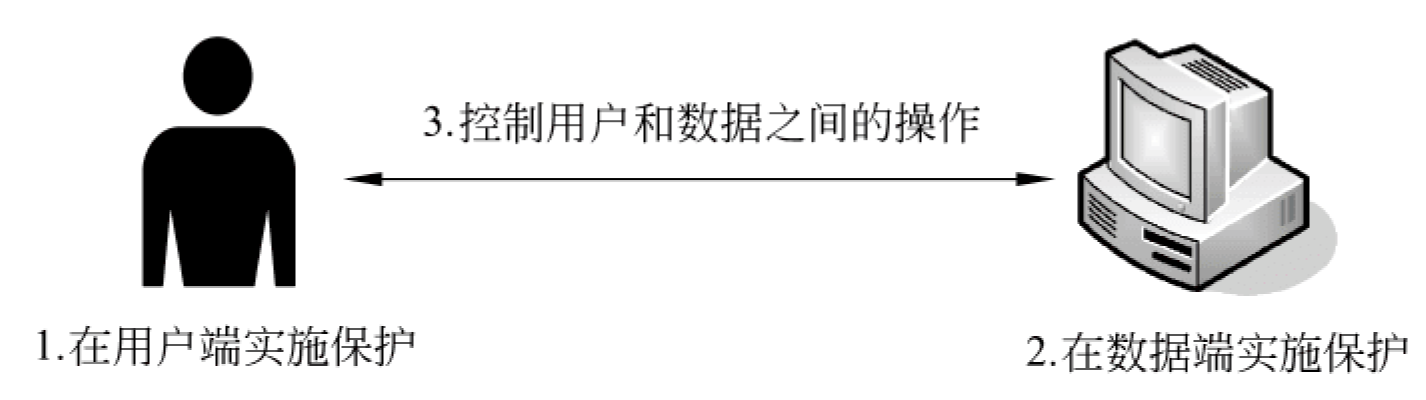


图5-1 安全机制设置的位置

一旦这些通用的问题确定以后,接下来就是确定安全机制设置在何处,它可以设置在硬件、内核、操作系统、服务或程序级。那么究竟将安全机制设置在哪一层?如果保护在硬件层实现,保护机制更简单,可提供广泛的通用的保护。越是层次向上升,越是增加复

杂性,而功能则更加专门和细粒度。最高层也最复杂,因为它直接向用户提供广泛的功能和选项。功能和安全复杂性增加,则越靠近用户。复杂性增加,则安全机制的级别越低。如图 5-2 所示。

安全机制越复杂,提供的安全保障越低。因为机制越复杂,要求安装、测试维护和使用者的技术越熟练。工具越复杂,差错的概率越大。从而增加了安全危害的几率。安全机制越复杂,越难对所有可能的情况进行测试。反之简单的机制不能提供一系列丰富的功能和选项,虽然它易于安装、维护、使用和测试。所以当设计一个系统时,对功能和保障要很好地折中,正确选择安全机制。

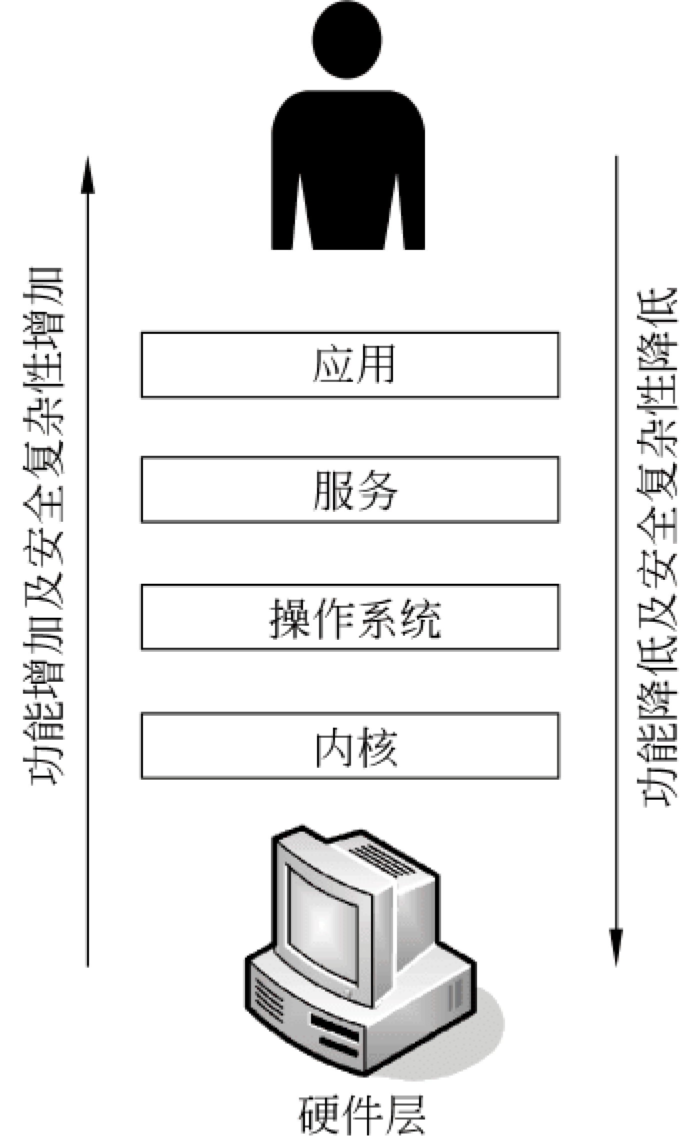


图 5-2　安全机制复杂性和安全保障的关系

一旦设计者选定了下面这些考虑:安全机制集中在用户、数据还是操作;安全机制放置在硬件、内核、操作系统,服务或程序哪一层;每个机制的复杂程度,就可以构建安全机制,并且和系统的其他部分用合适的方法集成起来。

第一步是决定什么样的系统机制需要可信的,以及说明这些实体如何以安全的方式交互。虽然要求系统内的所有部件都是可信的似乎更安全,但这会引入更多的开销、复杂性和性能瓶颈。对一个可信机制而言,它能保护自身及处理的数据,它以安全的、可预报的方式实现,不会对其他可信或不可信机制产生不利的影响。同时这些可信部件能访问更多的特权服务,能直接访问内存,当请求 CPU 处理时,有更高的优先级,以及对系统资源有更强的控制。因此,可信主体和客体需要被识别,和不可信主体能区别及放在一个指定的子集。

5.1.2　定义主体和客体的子集

如上所述,并非所有部件都必须是可信的,因此也不属于可信计算基(trusted computing base, TCB)。在计算机系统中全部保护机制的组合定义为 TCB。TCB 包括硬件、软件和固件。这些构成 TCB 的一部分,因为系统确信这些部件将实施安全策略并且不受侵犯。

需要识别 TCB 的各部件及定义它们可接受的能力。例如,一个低可信级别的系统允许所有授权用户访问和修改计算机上的所有文件。这样的主体和客体的集合很大,且它们间的关系是松散的、自由的。具有更高可信级别的系统可能只允许两个主体能访问计算机系统上的所有文件,而只有一个主体能修改所有的文件。这样的子集很小,且实施的规则更加严格和详细。

5.1.3　可信计算基

TCB 来源于美国国家计算机安全中心制定的橘皮书,在第 20 章安全认证和评估中将详细叙述。事实上没有一个计算机系统是完全安全的,因为攻击类型和漏洞随时会变

化，只要有足够的时间和资源，大部分攻击都能得逞。然而，如果一个系统满足一定准则，从安全角度看，似乎提供了一定的可信级别。

TCB 不只是对操作系统而言，因为一个计算机系统不只是由操作系统组成。TCB 涉及硬件、软件和固件，它们都可能正面地或负面地影响计算机环境，都有责任来支持和实施特定系统的安全策略。某些部件和机制在支持安全策略方面有直接的职责，如固件不让用户从软盘引导计算机，又如内存管理不让用户写其他用户的数据。有些部件不实施安全策略，但必须合适地运行，不侵犯系统的可信。侵犯一个部件的类型是多样的，可以引起系统安全策略的破坏，可以是一个应用程序企图直接调用某个硬件，而不是通过操作系统正常调用，可以是一个程序企图在允许的内存空间以外读数据，或者一些软件在使用一些资源后没有适当地释放资源。

并非系统的每个部分都需要是可信的，评估一个系统的可信级别是由构成 TCB 的结构、安全服务及保障机制确定的。要看 TCB 对于偶然的或故意的损害和破坏活动是如何保护的。对高可信级的系统必须满足严格定义的 TCB 要求，以及详细的运行状态、开发步骤、测试过程，更加细粒度的文本审查。

采用专门的安全准则，来构造、评估和验证可信系统，可以给客户提供一个度量标准，对不同的系统进行比较。同时给厂商提供指南，依据客户的安全要求生产合格的安全系统。

橘皮书定义了可信系统、系统的软件和硬件利用这个度量标准为不同用户集成不分类的和分类的数据，并且不违反访问权限和安全策略，在系统内所有的保护机制实施安全策略，提供期望的环境。这意味着系统的每一层必须信任下一层以执行预期的功能，提供期望的功能，在不同情况下以期望的方式运行。当操作系统调用硬件时，用专门的数据格式返回一个预期的数据，并且以一致的和预期的方式动作。运行在操作系统顶端的应用程序要求能作某种系统调用，接收需要的返回数据，能在可靠的环境中运行。用户期望硬件、操作系统、应用程序以特定的方式运行，并提供一定级别的功能。为了使所有这些能以预定的方式运行，系统的这些要求必须在开发的计划阶段就实施。

5.1.4 安全边界

如上所述，不是每个部件和资源都在 TCB 内，用安全边界来区分可信和不可信。某些资源不在 TCB 内即在安全边界外。当 TCB 内的部件需要和 TCB 外的部件通信，为了使系统处在可信和安全状态，必须开发精确的通信标准，以确保这种类型的通信不会带来非预期的安全危害。这类通信通过接口来处理和控制。

例如，在 TCB 安全边界内的资源不能将保密信息传给 TCB 外的资源。接收来自可信度较低资源的命令和信息，TCB 内的资源必须十分小心。这种限制是由实施安全边界的机制和允许这类通信发生的接口实现的，如图 5-3 所示。

在可信部件和非可信部件之间的通信必须加以控制，以确保保密信息不以非期望的方式流动。

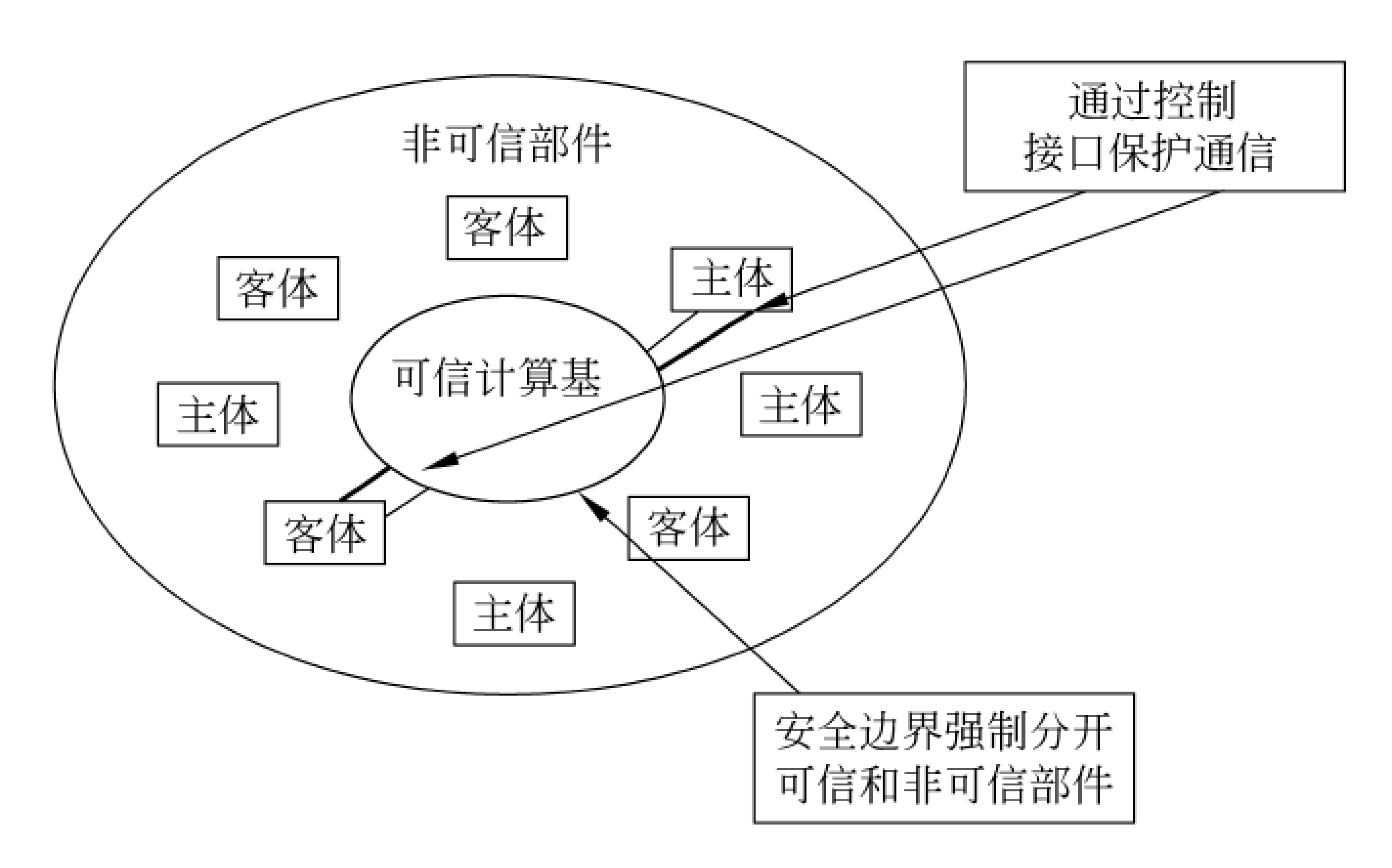


图 5-3　可信部件和非可信部件间通信的接口控制

5.1.5　基准监控器和安全内核

迄今为止，在开发计算机系统结构的任务中，已经定义了安全机制设置在何处（硬件、内核、操作系统、服务和程序）；定义了 TCB 内的客体，以及这些部件如何交互；构造了区分可信部件和非可信部件的安全周边，开发了合适的接口，使实体间安全通信。接下来需开发和实施一个机制，给予主体必要的允许权以访问客体。即需要开发和实施一个基准监控器和安全内核。基准监控器是一个抽象的机器，用来协调所有的访问主体和客体，以确保主体有必需的访问权，以及保护客体不被非授权访问、修改和破坏。对一个具有更高可信级的系统，必须给主体（程序、用户或进程）以优先授权来访问客体（文件、程序或资源）。基准监控器是一个访问控制概念，并非实在的物理部件，所以称它为基准监控器概念。安全内核由 TCB 内的一些机制构成，以实施和执行基准监控器概念。安全内核由硬件、固体和软件组成，以协调主体和客体间的访问及各种功能。安全内核是 TCB 的核心，是最常用的构造可信计算系统的方案：

- 为了执行基准监控器概念，它必须提供隔离且防篡改的功能。
- 对每个访问企图，基准监控器必须都行使其职责，且不可能被侵入。因此，基准监控器必须以完善的、十分安全的方法实行。
- 基准监控器必须是可验证的，这意味着所有基准监控器所做出的决定都应写成审计日志，并可验证。
- 它必须足够小，可以完善的、综合的方法进行测试和验证。

这些要求也是对提供和实施基准监控器概念的安全内核的要求。这些工作是抽象的，但是通过硬件设备和软件码的物理世界实现。实施基准监控器抽象概念的部件的保证是通过测试及其功能来证明的。

5.1.6　安全域

域定义为主体能访问的客体的集合。在这个域内的所有资源用户能访问，所有文件程序能用，内存段处理器能使用，以及各种服务和进程能被应用程序使用。一个主体需要能访问和使用客体（资源）来完成任务，域定义什么样的客体能被主体使用，什么样的客体

不能被主体使用。

这些域必须是能识别的、分开的，而且必须严格实施。操作系统可以工作在特权模式，也可以工作在用户模式。使用两种不同模式，可以定义两个不同的域。特权模式有更大的工作域，即更多资源可访问，因此也能提供更多的功能。当一个操作系统工作在特权模式，它能访问各个内存模块，能将数据从一个非保护域传送到保护域，且能和硬件设备直接访问和通信。工作在用户模式，应用程序不能直接访问内存，资源的应用也有更多限制。只有某些内存段可用于应用程序，且必须以非直接和受控的方式访问。应用仅能在自己的域内复制文件，且不能直接访问硬件。

存在于特权域的程序在执行指令和处理其数据时，必须保证不同域的程序不能负面影响其环境。因此称它为执行域（execution domain）。因为在特权域的程序要访问敏感资源，环境需要保护以防止其他域的程序产生的欺诈程序码或非预期的活动。某些系统仅有为数不多的用户和特权域，而有些系统恰有复杂的结构，甚至包含十多个安全域。

一个安全域和赋予主体或客体的保护环有直接的关联关系。越是小的保护环号，特权越高，安全域越大。这个概念如图 5-4 所示。

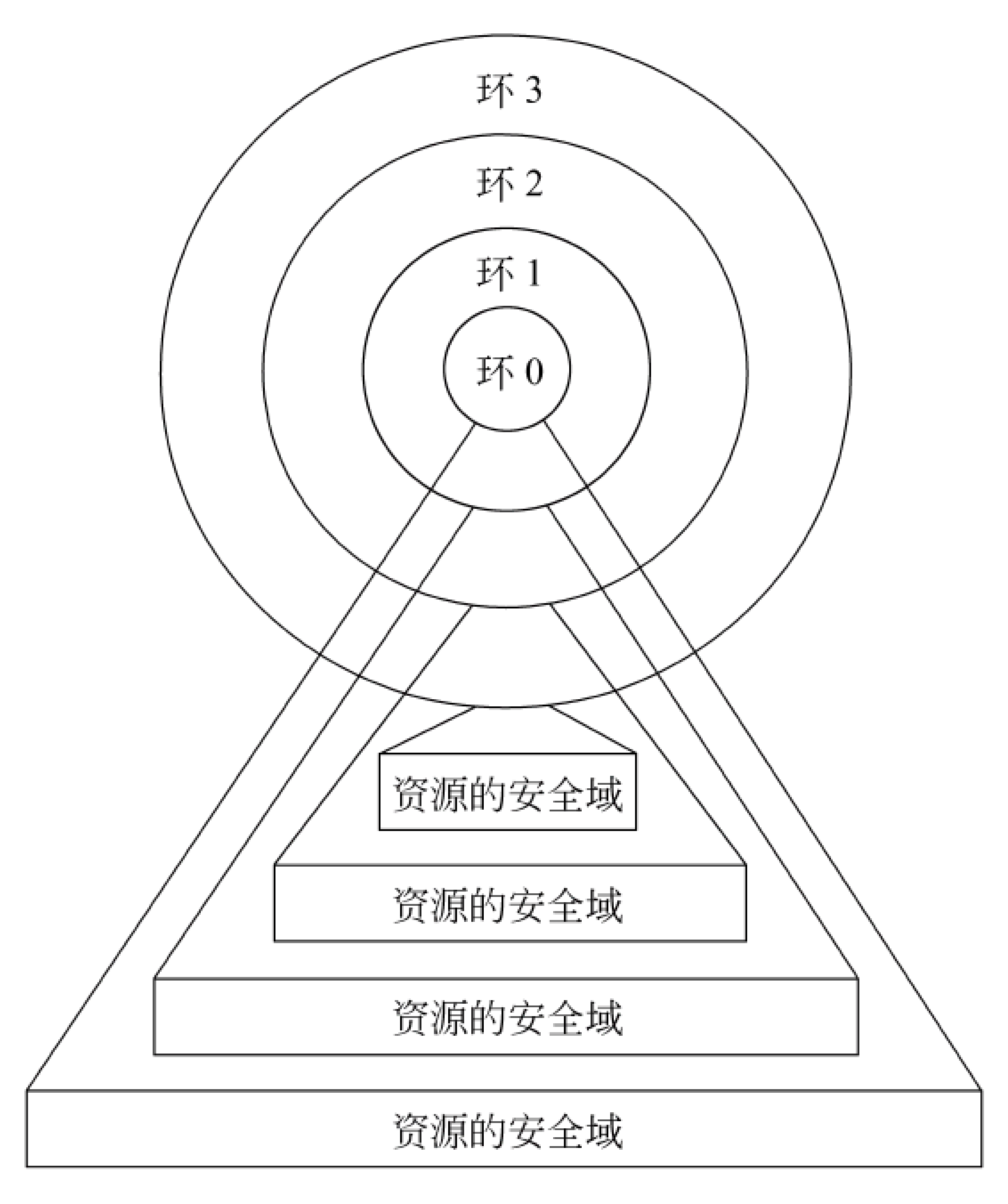


图 5-4　可信级和安全域的关系

5.1.7　资源隔离

为了正确实施访问控制、审计、决定什么样的主体和客体存在于专门的域，每个资源必须清楚地相互分开。模块化要求能使每个主体和客体可唯一识别、独立地赋予允许权，可审计的及复杂的活动能精确跟踪。主体、客体和保护控制需要清楚地相互隔离，而隔离的方法和实施是系统的体系结构及其安全模型的需求。

进程也是需要隔离的资源，通常通过不同的地址分配来实现。虚拟内存技术用来使

不同的进程有一个特殊的内存分配范围，它并不知道系统还有其他内存。进程随机地在分配的内存区内工作，不会影响其他内存段的其他进程数据。

对高可信级的系统，需要实施内存的硬件分段用于不同的进程。这意味着内存是物理上分开的，而不是逻辑上分开。这就增加了一层保护，确保较低特权的进程不会对较高级进程的内存空间进行存取和修改。

5.1.8　安全策略

前面提到 TCB 包含了直接实施安全策略的部件。什么是安全策略呢？安全策略是一些规则的集合，指明敏感信息是如何管理、保护和分布的。安全策略确切地表达要实现的安全机制的目标设置是何种级别。这在定义系统设计时是一个十分重要的目标。安全策略是系统规范的基础，提供评估系统的基准。在第 3 章已经详细讨论了安全策略，但重点是讲述一个组织的安全策略，而这里所指的是操作系统和应用程序的安全策略。

一个系统提供可信是通过符合和实施安全策略，典型的是处理主体和客体之间的关系。安全策略必须指明什么样的主体能访问什么样的客体，以及什么样的行为是可接受的或不可接受的。安全策略好似计算系统的框架，根据这些框架定义系统的可信。

为了提供一个可接受的可信级的系统，它必须基于体系结构，提供保护能力，以防止不可信的进程、不经意的或故意的危害，以及系统的不同层的攻击。大多数可信级别需要定义主体和客体的子集、清晰的各个域以及资源隔离，这样它们的访问能被控制，执行的活动能被审计。

综上所述，一个系统的可信是由准则的集合定义的。根据准则的集合测试一个系统，即可赋予这个系统的级别，并用于客户、厂商以至整个计算世界。准则将决定安全策略是否被支持和实施。安全策略设计各种规则以及实践有关系统如何管理、保护以及分布敏感信息。基准监控器是一个概念，即所有主体必须有合适的权力访问客体，并由安全内核实施。安全内核由根据系统安全策略管理系统活动的资源组成，是控制访问系统资源的操作系统的一部分。为了正确地工作，这些资源需要相互隔离，并且需要定义域来支配什么样的客体可被什么样的主体使用。

安全策略阻止信息从高安全级别流向低安全级别，称多级安全策略。这样的安全策略只有在主体安全级别高于或等于客体的安全类别时，主体才能访问客体。

这些抽象概念将体现到硬件、固件、软件码，以及设计、构造和实施系统的全过程中。

5.1.9　最小特权

一旦资源和进程被恰当地隔离，就需要实施最小特权。这意味着只需要为了满足其功能必需的特权。仅仅需要执行关键系统功能的进程被允许，而其他较少特权的进程只有当需要时才调用较高特权的进程来执行这些类型的活动。这种间接活动的类型保护了系统，以防止错误的或恶意的代码。进程需要占有特权的时间只是在真正需要的时候。当进程升高其特权级时，它就能直接和敏感信息交互，任务完成时，进程就应降低到较低特权级，以确保其他机制能使用，以防对系统产生有害的影响。只有需要完全特权的进程分布在内核，其他较低特权的进程调用它来处理敏感的操作。

5.1.10　分层、数据隐蔽和抽象

为满足一定的可信级，系统必须提供一种机制，使不同进程工作在不同层，即在系统的不同层产生不同的功能。这需要一个结构化的和层次的结构，使基本功能发生在较低层，而较复杂的、敏感的功能在较高层，分层结构进一步将进程和资源分开，在系统中加入模块化。层之间能够通信，但必须通过详细的接口，支持系统的安全集成。

在某些场合，要求不同层的进程不能通信，因此不提供相互通信的接口。这种进程称为数据隐蔽，在一个层的数据是隐蔽的，因为在其他层的主体并不知道该数据的存在。假如在一个层的主体没有接口能和另一层的数据通信，那么，该数据对那个主体是隐蔽的。

客体能组合成一个集合，称为类。当一类客体被赋予一定的允许权，定义可接受的活动，称为抽象。这使不同客体的管理更加容易，因为只需管理类，而不需对每个客体进行管理。当定义了一个类，所有在这个类内的客体被赋予一个抽象数据类型，它是客体接受数据及格式的格式化的精确定义，也是对其他客体和主体处理数据的表示。这提供了可预期的通信方式，有助于阻止授权实体用不正当的方法修改客体内的数据。例如，一个客体传递一个注册值给另一个客体，必须以预定的方式进行，接收的客体对超出预定边界的值不予接收。假如接收客体期望一个二进制值，则不会接收十六进制值。这种限制是在客体的抽象数据类型中定义的。

分层、数据隐蔽和抽象都是保护主体、客体及客体内的数据的方法。这些概念是安全模型的基本组成。

5.2　网络安全体系结构

因为漏洞可能在网络体系结构的不同层存在，厂商、开发人员、管理者，以及从事网络安全的专业人员有必要深入了解网络的各个层次，以及如何保护每个层。

我们经常听到网络安全的层次方案，也就是实施不同层的保护，对不同类型的攻击保护网络。什么是层次方案的真实含义呢？如何知道网络是否实施了层次保护计划？

为了对付所有可能的安全危害和漏洞以保护内部的和外部的网络，就要深入地研究和回答上述问题。为了保护网络环境，就需要真正了解环境，实施的补丁，不同厂商的应用软件和硬件的区别，以及攻击如何实施。要完成安全环境的过程是迂回曲折的，而且永无止境，重要的是深入全面地了解网络环境。

5.2.1　不同层次的安全

安全的层次结构是抽象的，必须在理论上予以表达，实际上予以实施。有时层次结构的含义是从网络不同的方面来实施的。范围是很广的，包括编程的码、使用的协议、操作系统、应用的配置，以及通过用户的行为和安全程序来管理、控制所有这些问题。层次结构表示在各层次设置屏障以防止攻击和威胁。仅仅在工作站上运行防病毒软件并非抵制病毒的层次结构。必须在每个工作站、文件服务器、邮件服务器，以及通过代理服务器实

施内容过滤才是抵制病毒的层次结构。这是层次结构的一个例子。

对文件访问提供保护的层次方案是怎样的呢？假如管理者将所有用户分成特定的组，并且指明哪些组能访问公司的一些文件，或不能访问另一些文件，仅仅是层次方案中的一步。合适的保护文件访问，对文件和注册访问控制表的配置需要对用户和用户组的访问权限有更加细粒度的控制。对不同用户要有严格的登录凭证策略，并且要强制执行。文件访问的监控和审计要能识别任何可疑的活动。此外还需提供各种物理安全的屏障，并和文件访问控制协同工作。

5.2.2　网络体系结构的观点

不同类型的漏洞、攻击、威胁存在于网络的不同层次。层次方案深入研究网络环境的各种技术及每一层次的每种技术的复杂性。IP 欺骗是在网络层的一种攻击，字典攻击则发生在应用层，通信窃听是在数据链路层和物理层，各种病毒的侵入则是在应用层。假如一个组织只是配置防火墙和严格的口令规则，仍有很多层次的漏洞可以被攻击。

很多时候，一些组织对安置的防火墙、入侵检测系统和防病毒软件过于信任，往往对管理员产生一种安全的假想，十分重要的是要看进入网络和从网络出来的数据流，以及这些应用程序和设备是如何配合工作的。这是两种不同的观点，一种是网络体系结构的观点，另一种只是单纯的设备或应用程序的观点。

从体系结构的观点，必须观察出入的数据流及这些数据是如何授权，在不同的点是如何监控的，以及在不同的场合安全解决方案是如何协同工作的。例如，防火墙仅仅是全部体系结构的一部分，必须要有合适的层次安全结构，而不只是防火墙。好比一个好的管弦乐队需要配合协调演奏。即使每个单个安全部件能保护网络的某个部分很好工作，也不能确保这些安全部件一起工作时相互联系和通信时不产生问题。

每个网络环境因其安装的硬件、软件、技术和配置的不同而有所区别。然而各个环境的主要区别在于要达到的目标不同。局域网提供身份认证、用户资源及内部控制。广域网提供用户和远程站点的连接、协议转换及访问控制。电子商务系统提供 Internet 用户到 Web 的接口，后端服务器的数据连接，访问控制及和 LAN，WAN 不同的身份认证。这些不同的目标需要用不同的体系结构，但是能使用相同的、基本的安全概念。

图 5-5 表示在网络体系结构中不同的层次可能发生的攻击、漏洞及防护。

- 防火墙配置了分组过滤，这是在网络层提供防护，它抵御拒绝服务攻击和碎片攻击。
- 代理软件配置保护应用层，它抵御非授权访问攻击和分组欺骗攻击。
- 网络地址转换（NAT）工作在网络层，可以隐藏 LAN 的 IP 地址和拓扑。
- 屏蔽双绞线（STP）工作在物理层，它可以防止网络窃听和信号干扰。
- 网络入侵检测在网络层监控已知的攻击信号，它识别已知的攻击，并在必要时重新设置 TCP 连接。
- 周边域名服务器保存了资源记录，这是在应用层进行防护。它保护专用域名服务器记录、网络映射及各个计算机的信息。
- IPSec 工作在网络层，为虚拟专用网（VPN）连接到周边网而配置，可以为 IP 网络

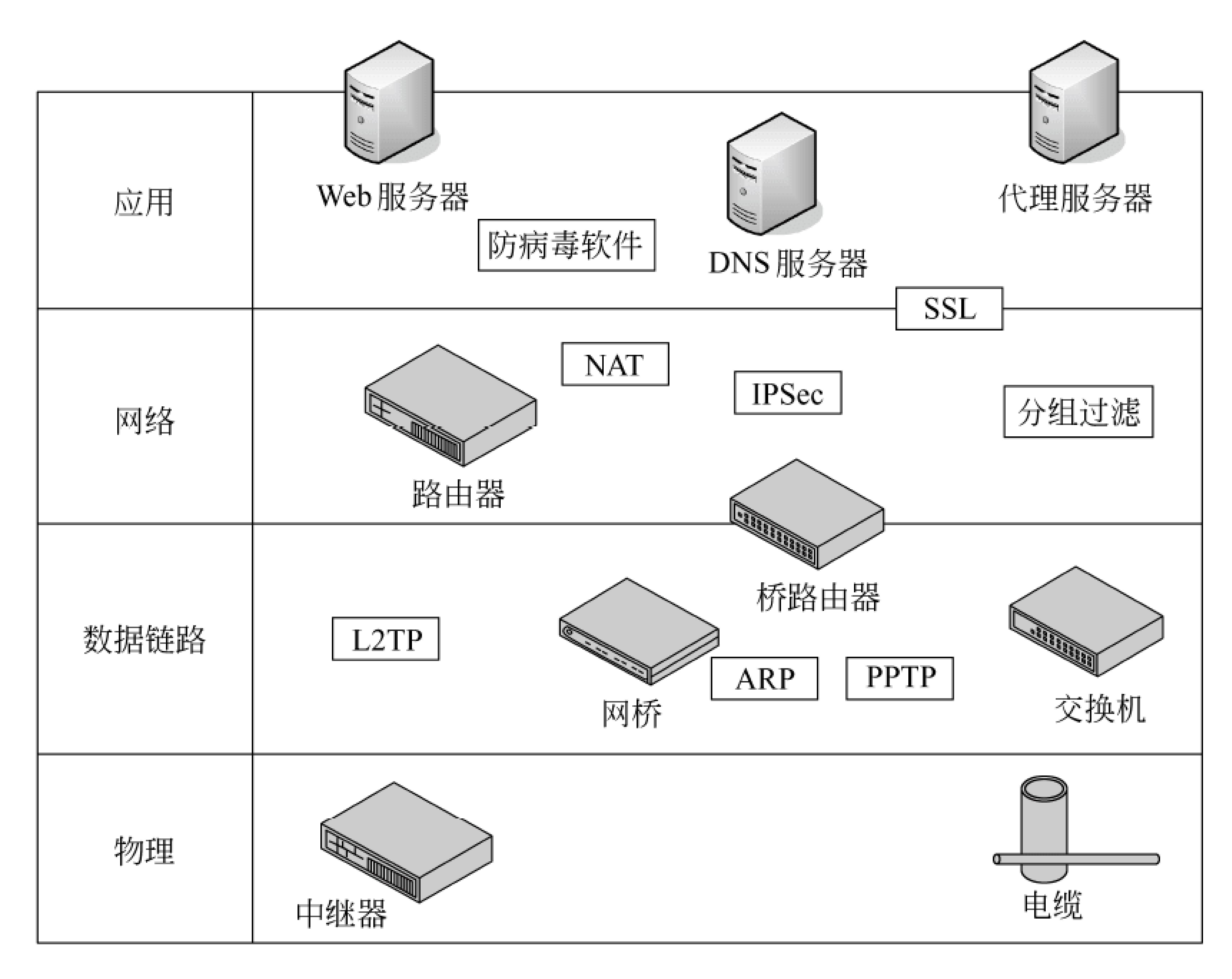


图 5-5　网络体系结构不同层次的安全防护

通信提供透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，保证数据的完整性和机密性，有效抵御网络攻击。

- 对公共信息和保密信息使用不同的服务器进行 Web 服务器的配置是在应用层进行保护，以抵御目录的非授权访问。
- 对所有周边设备仅仅提供必要的服务和端口使用，这是工作在网络层。从而减少了网络进入点，抵御拒绝服务攻击。
- 邮件服务器使用存储转发报文及在应用层运行防病毒软件，这是抵御病毒和拒绝服务攻击。
- 安全套接字层（SSL）工作在传输层，当客户需要从 Web 站点访问个人保密信息，可在 Web 站点配置 SSL。
- 网络扫描器对全部周边网络服务器端口每周进行扫描，以识别新的漏洞，这是工作在数据链路层和网络层。这是防护由于配置改变或引入新的技术而引起的新的漏洞。
- 工作在应用层的 Web 服务器，对扩展标记语言（extensible markup language，XML）码和分布部件目标模型（distributed component object model，DCOM）的安全使用嵌入式密码。这是提供信息的安全以及限制部件执行冒险动作。
- 工作在应用层和表示层的 Web 服务器需要提供数字签名以确保相互间的合法通信。这是抵御黑客攻击和各种欺骗。

上面只是列举了在网络层次模型的不同点上可能发生的很少一部分事件。假如有一个或更多的设备或软件有不正确的配置，假如网络环境失去上述各组成成分之一，就为黑

客攻击网络提供可乘之机。

很多环境并不包含全部上述列出的对各种安全漏洞的解决方案及设备，这就为精明的黑客提供了攻击的可能。下面是一个实例，在这个环境里已经设置的安全防御措施有以下一些：

分组过滤的防火墙，内容过滤的代理服务器，公共的和专用的 DNS 记录清楚地分开，SSL 用于 Internet 用户，IPSec 用于 VPN 连接，基础设施 PKI，以及严格限制的服务和端口配置。看上去这是一个具有坚固的安全防御的环境，网络管理员似乎用最完美的意图来实现这些安全机制。然而，这种坚固的防御环境仅仅是暂时的，如果没有漏洞检测设备定期监视这个环境或没有入侵检测系统寻找可疑的行为，即使公司花了大量的资金用于安全防御措施，这个环境仍有可能受攻击。技术在不断变化，网络环境也随之而改变，新的应用配置、补丁的应用、新的设备安装都会引起意想不到的后果，意识不到这些，黑客就会找到对付原始的安全机制的办法。

5.3 OSI 安全体系结构

OSI 安全体系结构的研究始于 1982 年，于 1988 年完成，其成果标志是 ISO 发布了 ISO 7498-2 标准，作为 OSI 基本参考模型的补充。这是基于 OSI 参考模型的七层协议之上的信息安全体系结构。它定义了 5 类安全服务、8 种特定的安全机制、5 种普遍性安全机制。它确定了安全服务与安全机制的关系，以及在 OSI 七层模型中安全服务的配置。它还确定了 OSI 安全体系的安全管理。

5.3.1 OSI 安全体系结构的 5 类安全服务

1. 鉴别

鉴别服务提供对通信中的对等实体和数据来源的鉴别，分述如下。

(1) 对等实体鉴别

确认有关的对等实体是所需的实体。这种服务由 N 层提供时，将使 N+1 层实体确信与之打交道的对等实体正是它所需要的 N+1 实体。

这种服务在连接建立或在数据传送阶段的某些时刻提供使用，用以证实一个或多个连接实体的身份。使用这种服务可以(仅仅在使用时间内)确信：一个实体此时没有试图冒充(一个实体伪装为另一个不同的实体)别的实体，或没有试图将先前的连接作非授权的重放(出于非法的目的而重新发送截获的合法通信数据项的备份)；实施单向或双向对等实体鉴别也是可能的，可以带有效期检验，也可以不带。这种服务能够提供各种不同程度的鉴别保护。

(2) 数据原发鉴别

确认接收到的数据的来源是所要求的。这种服务当由 N 层提供时，将使 N+1 实体确信数据来源正是所要求的对等 N+1 实体。数据原发鉴别服务对数据单元的来源提供

确认。这种服务对数据单元的重放或篡改不提供鉴别保护。

2. 访问控制

防止对资源的未授权使用，包括防止以未授权方式使用某一资源。这种服务提供保护以对付开放系统互连可访问资源的非授权使用。这些资源可以是经开放系统互连协议访问到的 OSI 资源或非 OSI 资源。这种保护服务可应用于对资源的各种不同类型的访问（如使用通信资源、读写或删除信息资源、处理资源的操作），或应用于对某种资源的所有访问。

这种访问控制要与不同的安全策略协调一致。

3. 数据机密性

这种服务对数据提供保护，使之不被非授权地泄露。具体分为以下几种：

（1）连接机密性

这种服务为一次 N 连接上的全部 N 用户数据保证其机密性。但对于某些使用中的数据，或在某些层次上，将所有数据（例如加速数据或连接请求中的数据）都保护起来反而是不适宜的。

（2）无连接机密性

这种服务为单个无连接的 N-SDU（N 层服务数据单元）中的全部 N 用户数据提供机密性保护。

（3）选择字段机密性

这种服务为那些被选择的字段保证其机密性，这些字段或处于 N 连接的 N 用户数据中，或为单个无连接的 N-SDU 中的字段。

（4）通信业务流机密性

这种服务提供的保护，使得无法通过观察通信业务流推断出其中的机密信息。

4. 数据完整性

这种服务对付主动威胁。在一次连接上，连接开始时使用对某实体的鉴别服务，并在连接的存活期使用数据完整性服务就能联合起来为在此连接上传送的所有数据单元的来源提供确证，为这些数据单元的完整性提供确证，例如，使用顺序号可为数据单元的重放提供检测。数据完整性可分为以下几种：

（1）带恢复的连接完整性

这种服务为 N 连接上的所有 N 用户数据保证其完整性，并检测整个 SDU 序列中的数据遭到的任何篡改、插入、删除或同时进行补救或恢复。

（2）无恢复的连接完整性

与上款的服务相同，只是不做补救或恢复。

（3）选择字段的连接完整性

这种服务为在一次连接上传送的 N-SDU 的 N 用户数据中的选择字段保证其完整性，所取形式是确定这些被选字段是否遭受了篡改、插入、删除或不可用。

（4）无连接完整性

这种服务当由 N 层提供时，对发出请求的那个 N+1 实体提供了完整保护。

这种服务为单个的无连接的 SDU 保证其完整性，所取形式可以是一个接收到的 SDU 是否遭受了篡改。此外，在一定程度上也能提供对连接重放的检测。

(5) 选择字段无连接完整性

这种服务为单个连接上的 SDU 中的被选字段保证其完整性，所取形式为被选字段是否遭受了篡改。

5. 抗否认

这种服务可取如下两种形式，或两者之一：

(1) 有数据原发证明的抗否认

为数据的接收者提供数据的原发证据。这将使发送者不承认未发送过这些数据或否认其内容的企图不能得逞。

(2) 有交付证明的抗否认

为数据的发送者提供数据交付证据。这将使接收者事后不承认收到过这些数据或否认其内容的企图不能得逞。

5.3.2　OSI 安全体系结构的安全机制

1. 特定的安全机制

本节所列的 8 种安全机制可以设置在适当的 N 层上，以提供 OSI 安全体系结构的某些安全服务，分述如下。

(1) 加密机制

对数据进行密码变换以产生密文。加密可以是不可逆的，在这种情况下，相应的解密过程便不能实现了。

① 加密既能为数据提供机密性，也能为通信业务流信息提供机密性，并且是其他安全机制中的一部分或对安全机制起补充作用。

大多数应用不要求在多个层加密，加密层的选取主要取决于下列几个因素：

- 如果要求全通信业务流机密性，那么将选取物理层加密，或传输安全手段(如适当的扩频技术)。足够的物理安全，可信任的路由选择及在中继上的类似机制能够满足所有的机密性要求。
- 如果要求细粒度保护(即对不同应用提供不同的密钥)，和抗否认或选择字段保护，那么将选取表示层加密。由于加密算法耗费大量的处理能力，所以选择字段保护是很重要的。在表示层中的加密能提供不带恢复的完整性、抗否认以及所有的机密性。
- 如果希望实现所有端系统到端系统通信的简单块保护，或希望有一个外部的加密设备(例如，为了给算法和密钥加物理保护，或防止错误软件)，那么将选取网络层加密。这能够提供机密性与不带恢复的完整性。虽然在网络层不提供恢复，但传输层的正常的恢复机制能够恢复网络层检测到的攻击。
- 如果要求带恢复的完整性，同时又具有细粒度保护，那么将选取传输层加密。这

能提供机密性、带恢复的完整性或不带恢复的完整性。

• 对于今后的实施，不推荐在数据链路层上加密。

当关系到这些主要因素中的两项或多项时，可能需要在多个层上提供加密。

② 加密算法可以是可逆的，也可以是不可逆的。

可逆加密算法有两大类：

• 对称(即秘密密钥)加密。对于这种加密，知道了加密密钥也就意味着知道了解密密钥；反之亦然。

• 非对称(即公开密钥)加密。对于这种加密，知道了加密密钥并不意味着也知道了解密密钥；反之亦然。

不可逆加密算法可以使用密钥，也可以不使用。若使用密钥，密钥可以是公开的，也可以是秘密的。

③ 除了某些不可逆加密算法的情况外，加密机制的存在便意味着要使用密钥管理机制。密钥管理方法上的一些准则将在第 18 章中给出。

(2) 数字签名机制

数字签名是附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者确认数据单元来源和数据单元的完整性，并保护数据，防止被人(例如接收者)伪造。

数字签名机制确定两个过程：对数据单元签名、验证签过名的数据单元。

第一个过程使用签名者所私有的(即独有的和机密的)信息。第二个过程所用的规程与信息是公之于众的，但不能从它们推断出该签名者的私有信息。

数字签名机制具有如下特点：

① 签名过程使用签名者的私有信息作为私钥，或对数据单元进行加密，或产生出该数据单元的一个密码校验值。

② 验证过程使用公开的规程与信息来决定该签名是否是用签名者的私有信息产生的。

③ 签名机制的本质特征为该签名只有使用签名者的私有信息才能产生出来。因而，当该签名得到验证后，它能在事后的任何时候向第三方(例如法官或仲裁人)证明只有那个私有信息的唯一拥有者才能产生这个签名。

(3) 访问控制机制

为了决定和实施一个实体的访问权，访问控制机制可以使用该实体已鉴别的身份，或使用有关该实体的信息(例如它与一个已知的实体集的从属关系)，或使用该实体的权利。如果这个实体试图使用非授权的资源，或者以不正当方式使用授权资源，那么访问控制功能将拒绝这一企图，另外还可能产生一个报警信号或记录它作为安全审计跟踪的一个部分来报告这一事件。对于无连接数据传输，发给发送者的拒绝访问的通知只能作为强加于原发的访问控制结果而被提供。

访问控制机制可以使用下列一种或多种手段。

① 访问控制信息库：保存对等实体的访问权限。信息可以由授权中心保存，或由正被访问的那个实体保存。信息的形式可以是一个访问控制表，或是等级结构的矩阵。使

用这一手段要预先假定对等实体的鉴别已得到保证。

② 鉴别信息：例如口令，对这一信息的占有和出示便证明正在进行访问的实体已被授权。

③ 权利：对它的占有和出示便证明有权访问由该权利所规定的实体或资源，权利应是不可伪造的并以可信赖的方式进行运送。

④ 安全标记：当与一个实体相关联时，这种安全标记可用来表示同意或拒绝访问，通常根据安全策略而定。

访问控制机制可应用于通信联系中的端点，或应用于任一中间点。涉及原发点或任一中间点的访问控制，是用来决定发送者是否被授权与指定的接收者进行通信，或是否被授权使用所要求的通信资源。

在无连接数据传输目的端上的对等级访问控制机制的要求在原发点必须事先知道，还必须记录在安全管理信息库中。

(4) 数据完整性机制

数据完整性有两个方面：单个数据单元或字段的完整性和数据单元流或字段流的完整性。一般来说，用来提供这两种类型完整性服务的机制是不相同的。

决定单个数据单元的完整性涉及两个过程，一个在发送实体上，一个在接收实体上。发送实体给数据单元附加一个量，这个量为该数据的函数。这个量可以是分组校验码那样的补充信息，或是一个密码校验值，而且它本身可以被加密。接收实体产生一个相应的量，确定这个量中的数据是否在传送中被篡改过。单靠这种机制不能防止单个数据单元的重放。在网络体系结构的适当层上，操作检测可能在本层或较高层上起到恢复作用(例如，重传或纠错)。

对于连接方式数据传送，保护数据单元序列的完整性(即防止乱序、数据的丢失、重放、插入或篡改)另外还需要某种明显的排序形式，如顺序号、时间标记或密码链。

对于无连接数据传送，时间标记可以用来在一定程度上提供保护，防止个别数据单元的重放。

(5) 鉴别交换机制

可用于鉴别交换的一些技术：使用鉴别信息(例如口令)，由发送实体提供而由接收实体验证；密码技术；使用该实体的特征或占有物。

这种机制可设置在 N 层以提供对等实体鉴别。如果在鉴别实体时，这一机制得到否定的结果，就会导致连接的拒绝或终止，也可能使在安全审计跟踪中增加一个记录，或给安全管理中心一个报告。

当采用密码技术时，这些技术可以与“握手”协议结合起来以防止重放(即确保存活期)。

鉴别交换技术的选用取决于使用它们的环境。在许多场合，它们必须与下列各项结合使用：时间标记与同步时钟；双方握手和三方握手(分别对应于单方鉴别和相互鉴别)；由数字签名和公证机制实现的抗否认服务。

(6) 通信业务填充机制

通信业务填充机制能用来提供各种不同级别的保护，对抗通信业务分析。这种机制

只有在通信业务填充受到机制服务保护时才是有效的。

(7) 路由选择控制机制

路由选择控制机制具有以下特点：

① 路由能动态地或预定地选取，以便只使用物理上安全的子网络、中继站或链路。

② 在检测到持续的操作攻击时，端系统可以指示网络服务的提供者经不同的路由建立连接。

③ 带有某些安全标记的数据可能被安全策略禁止通过某些子网络、中继站或链路。连接的发起者(或无连接数据单元的发送者)可以指定路由选择说明，由它请求回避某些特定的子网络、中继站或链路。

(8) 公证机制

有关在两个或多个实体之间通信的数据的性质，如它的完整性、原发、时间和目的地等能够借助公证机制得到确保。这种保证是由第三方公证人提供的。公证人为通信实体所信任，并掌握必要信息以一种可证实方式提供所需的保证。每个通信事例可使用数字签名、加密和完整性机制以适应公证人提供的那种服务。当这种公证机制被用到时，数据便在参与通信的实体之间经由受保护的通信实体和公证方进行通信。

2 普遍性安全机制

普遍性安全机制不是为任何特定的服务而特设的，因此，在任一特定的层上，对它们都不作明确的说明。某些普遍性安全机制可认为属于安全管理方面。普遍性安全机制可分为以下几种。

(1) 可信功能度

可信功能度可以扩充其他安全机制的范围，或建立这些安全机制的有效性；可以保证对硬件与软件寄托信任的手段已超出本标准的范围，而且在任何情况下，这些手段随已察觉到的威胁的级别和被保护信息的价值而改变。一般说来，这些手段的代价高而且难以实现。解决办法是选取一个体系结构，它允许安全功能在一些模块中实现，这些模块能与非安全功能分开来制作，并由非安全功能来提供。

应用于一个层而对该层之上的联系所作的任何保护必须由另外的手段来提供，例如通过适当的可信功能度。

(2) 安全标记

安全标记是与某一资源(可以是数据单元)密切相关联的标记，为该资源命名或指定安全属性(这种标记或约束可以是明显的，也可以是隐含的)。

包含数据项的资源可能具有与这些数据相关联的安全标记，例如指明数据敏感性级别的标记。常常必须在传送中与数据一起运送适当的安全标记。安全标记可能是与被传送的数据相连的附加数据，也可能是隐含的信息。例如，使用一个特定密钥加密数据所隐含的信息，或由该数据的上下文所隐含的信息。明显的安全标记必须是清晰可辨的，以便对它们作适当的验证。此外，它们还必须安全可靠地依附于与之关联的数据。

(3) 事件检测

与安全有关的事件检测包括对安全明显事件的检测，也可以包括对“正常”事件的检

测，例如，一次成功的访问(或注册)。与安全有关的事件的检测可由 OSI 内部含有安全机制的实体来做。构成一个事件的技术规范由事件处置管理来维护。对各种安全事件的检测，可能引起一个或多个如下动作：在本地报告这一事件；远程报告这一事件；对事件作记录；进行恢复。这种安全事件的例子为：特定的安全侵害；特定的选择事件；对事件发生次数计数的溢出。

这一领域的标准化将考虑对事件报告与事件记录有关信息的传输，以及为了传输事件报告与事件记录所使用的语法和语义的定义。

(4) 安全审计跟踪

安全审计就是对系统的记录与行为进行独立的评估考查，目的是测试系统的控制是否恰当，保证与既定策略和操作的协调一致，有助于做出损害评估，以及对在控制、策略与规程中指明的改变做出评价。其目的在于：

① 安全审计跟踪提供了一种不可忽视的安全机制，它的潜在价值在于经事后的安全审计可以检测和调查安全的漏洞。安全审计要求在安全审计跟踪中记录有关安全的信息，分析和报告从安全审计跟踪中得来的信息。这种日志或记录被认为是一种安全机制并予以描述，而把分析和报告视为一种安全管理功能。

② 搜集审计跟踪的信息，通过列举被记录的安全事件的类别(例如对安全要求的明显违反或成功操作的完成)，能适应各种不同的需要。安全审计可对某些潜在的侵犯安全的攻击源起到威慑作用。

③ OSI 安全审计跟踪将考虑要选择记录什么信息、在什么条件下记录信息，以及为了交换安全审计跟踪信息所采用的语法和语义定义。

(5) 安全恢复

安全恢复处理来自诸如事件处置与管理功能等机制的请求，并把恢复动作当作应用一组规则的结果。恢复动作可能有 3 种：立即动作，可能造成操作的立即放弃，如断开；暂时动作，可能使一个实体暂时无效；长期动作，可能是把一个实体记入“黑名单”，或改变密钥。

对于标准化的课题包括恢复动作的协议，以及安全恢复管理的协议。

5.3.3　三维信息系统安全体系结构框架

一个三维的信息系统安全体系结构框架反映了信息系统安全需求和体系结构的共性，如图 5-6 所示。

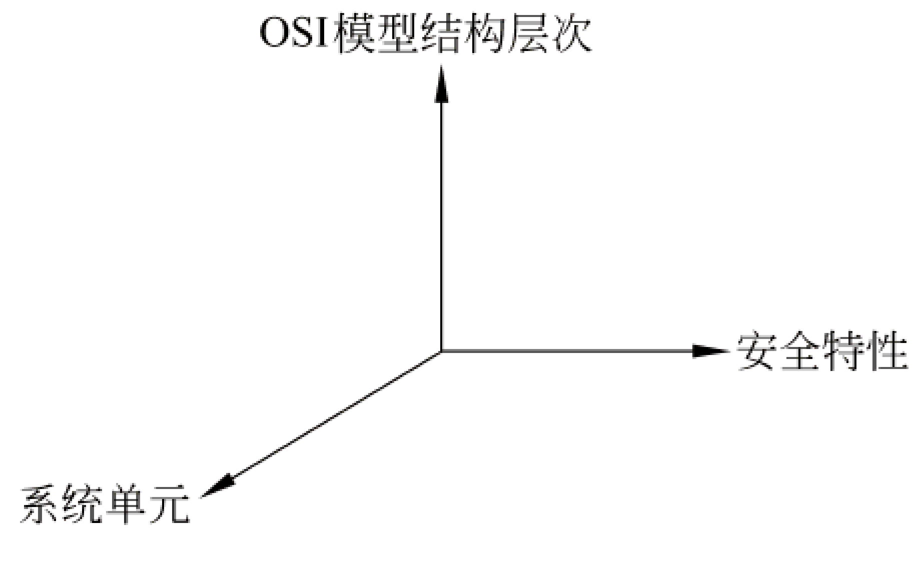


图 5-6　信息系统安全体系结构框架

图中的三维特性分别是安全特性、系统单元及开放系统互连参考模型。

安全特性是基于 ISO 7498-2 的 5 种安全服务，包括身份鉴别、访问控制、数据保密、数据完整、不可抵赖，以及审计管理及可用性。不同的安全政策、不同安全等级的系统可有不同的安全特性需求。

系统单元包括信息处理单元、网络系统、安

全管理及物理和行政的环境。信息处理单元由端系统和中继系统(网桥、路由器等)组成。端系统的安全体系结构要支持具有不同政策的多个安全域,安全域是指用户、用户的信息客体及安全策略的集合。通过物理和行政的安全管理体制提供安全的本地用户环境以保护硬件;通过防干扰、防辐射、容错、检错等手段实现硬件对软件的保护;提供用户身份认证、访问控制等机制实现软件对信息的保护。

通信网络的安全为传输中的信息提供保护,支持信息共享和分布处理。通信网络系统安全支持包括安全通信协议、密码支持、安全管理应用进程、安全管理信息库和分布式管理系统等。通信网络安全要提供开放系统通信环境下的通信业务流安全。

ISO 7498-2 制定了有关安全管理的机制,包括安全域的设置和管理、安全管理信息库、安全管理信息的通信、安全管理应用程序协议及安全机制与服务管理。

物理环境与行政管理安全包括人员管理与物理环境管理、行政管理与环境安全服务配置和机制及系统管理员职责等。

5.4　ISO/IEC 网络安全体系结构

5.4.1　ISO/IEC 安全体系结构参考模型

ISO(The International Organization for Standardization)和 IEC(The International Electrotechnical Commission)18028-2 定义了一个标准安全结构,描述支持网络安全规划、设计和实施的一致框架,以提供端到端的网络安全。该结构能应用到考虑端到端安全的各种网络,并独立于网络的实施技术。

定义网络安全参考结构应对服务提供者、企业、消费者所面临的全球安全挑战,可适用于任何类型的现代网络,包括无线、光纤、语音、数据和综合业务网,关注网络基础设施、服务和应用的管理、控制和使用的安全。参考结构提供了一个综合的、自上而下的、端到端的网络安全视角,能应用到各种综合的网络部件、服务和应用以预测、检测和校正网络脆弱性。

参考结构将一组复杂的端到端网络安全相关的特性逻辑上分解成各个结构组成,从而生成端到端安全的有序的方案,既可用于评估生成现存网络的安全,也可用于规划新的安全方案。

安全体系结构参考模型由 3 个结构组件构成:

- 安全维 (security dimensions);
- 安全层 (security layers);
- 安全面 (security planes)。

1. 安全维

在风险管理进程中,确定合适的安全度量来管理或缓解评估的风险,安全维列出了一组安全度量,这些安全度量用于实施网络安全的某一特定方面的安全控制措施。安全维的概念不仅限于网络,对相关的应用或最终用户也是有用的。安全维包括以下 8 个方面:

① 访问控制;

② 身份鉴别；

③ 不可否认；

④ 数据保密；

⑤ 通信流安全；

⑥ 数据完整性；

⑦ 可用性；

⑧ 隐私。

合适的设计和实施安全维来支持安全策略，而安全策略是对特定的网络和设施定义的一组规则的集合，并用于安全管理。

2 安全层

为了提供端到端的安全解决方案，安全维必须应用到网络设备和设施的层次结构上，称为安全层。参考安全体系结构定义了 3 个层：

① 基础设施安全层；

② 服务安全层；

③ 应用安全层。

安全层提供网络安全的层次解决方案，基础设施安全层支持服务安全层，而服务安全层支持应用安全层。参考安全体系结构论述了每个层有不同的安全脆弱性以及各种潜在的安全威胁。安全层的含义和 OSI 有关，但是有不同的含义。

安全层表示在产品的何处必须考虑安全，并且提供网络的有序解决方案。例如，首先考虑基础设施安全层的安全脆弱性，然后是服务安全层，最后才是应用安全层的安全脆弱性。而安全维是在每个安全层需要解决的范围。图 5-7 表示每个安全维的机制如何应用到安全层，以降低每层的脆弱性，从而缓解安全攻击。

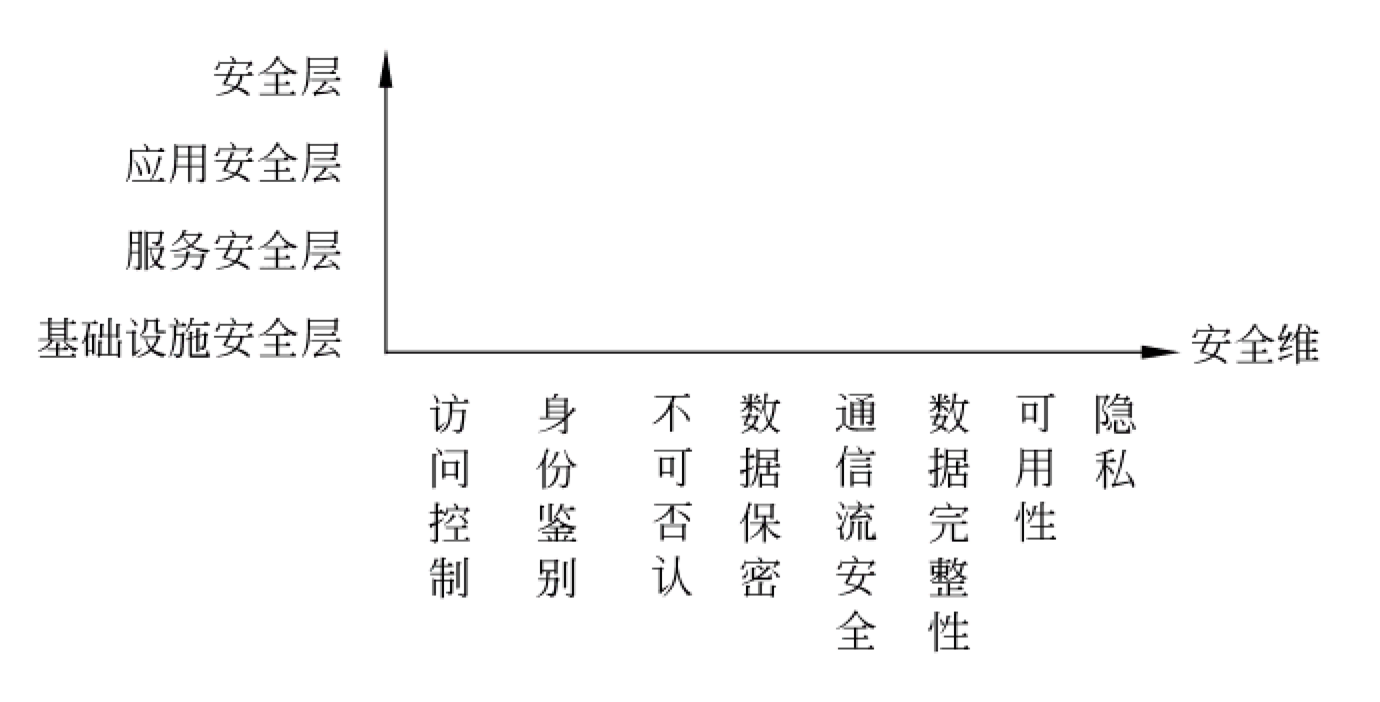


图 5-7　安全维应用到安全层

基础设施安全层由网络传输设备和各个网络部件组成，后者由实施安全维的机制保护。基础设施安全层包括网络的基本组成部件及其服务和应用。例如，属于基础设施安全层的组件是各个路由器、交换机、服务器及在各个路由器、交换机和服务器之间的通信链路。

服务安全层涉及服务提供者给客户提供的服务安全。这些服务包括从基本的传输和连接服务到为了提供 Internet 访问必需的一些服务（也就是身份鉴别、授权、账户服务、动

态主机配置服务和域名服务等），以及诸如 VPN、QoS 等增值服务。服务安全层用来保护服务提供者及其客户，两者都是安全威胁的可能目标。例如，攻击者企图拒绝服务提供者提供服务的能力，或者企图破坏服务提供者的一些客户的服务。应用安全层集中在服务提供者客户访问的基于网络应用的安全。这些应用包括基本的文件传送 FTP 和 Web 浏览应用，诸如目录帮助、基于网络的语音消息和电子邮件等基本应用，以及诸如客户关系管理、电子商务、基于网络的培训和视频合作等高端应用。基于网络的应用可以由第三方应用服务提供者（ASPs）提供。在这层有 4 个安全攻击的潜在目标，包括应用用户、应用提供者、由第三方集成者提供的中间件及服务提供者。

3. 安全面

安全面是为实施安全维的机制所保护的某种类型的网络活动。参考结构定义了 3 个安全面，表示作用在网络的 3 种保护活动的类型：

① 管理安全面；

② 控制安全面；

③ 最终用户安全面。

这些安全面涉及和网络管理活动、网络控制或信令活动及最终用户相关的活动的特定的安全需求。

网络应该设计成一个安全面的活动尽可能独立于另一个安全面的活动。例如，由最终用户请求引起的最终用户安全面的 DNS 查找的淹没不应该锁住管理安全面的 OAM/SP 接口，从而允许管理者来处理该问题。

图 5-8 表示包括各安全面的参考结构，每种网络安全活动有其特定的安全需求。安全面的概念允许对相关的活动和能力的独立性考虑特定的安全的差异。例如，VoIP 服务是由服务安全层处理，而 VoIP 服务的管理安全是独立于服务的控制安全（诸如 SIP 协议），也独立于最终用户要传送的数据（即用户的声音）的安全。

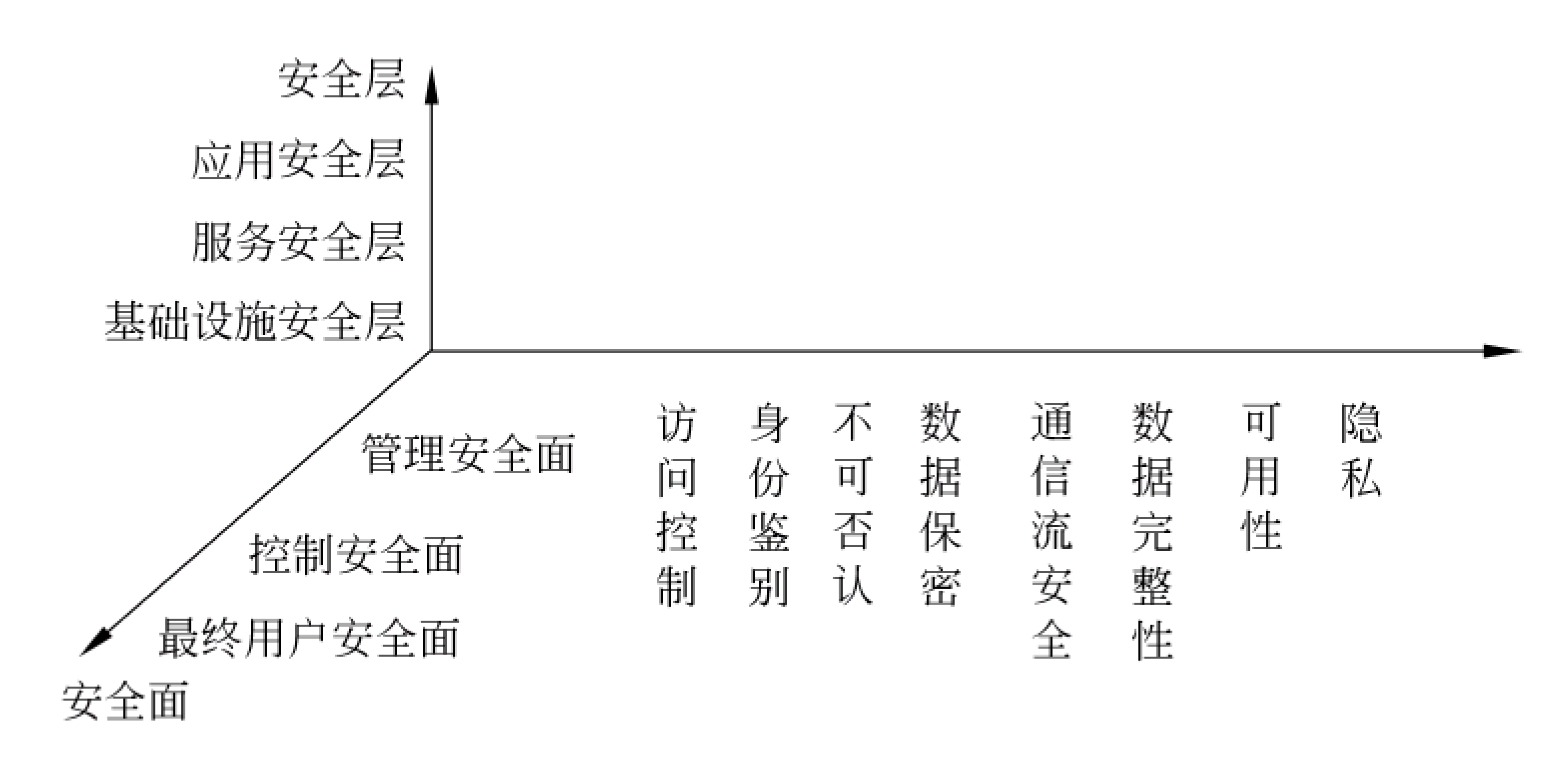


图 5-8　反映不同网络活动类型的安全面

管理安全面是考虑保护各网络部件传输设施、后备系统（运行支持系统、业务支持系统、客户提示系统）及数据中心的 OAM/SP 功能。管理安全面支持故障、能力、管理、规定和安全功能。控制安全面是考虑保护能在网上有效传递信息、服务和应用的活动。例如，对机器到机器的信息通信应允许路由器、交换机决定如何在传输网上最佳的路由和交

换通信。这类信息常常归结为控制或信令信息。网络携带这类信息可以是进入的(in-band),或出去的(out-of-band),表示服务提供者的用户通信。这些类型的信息包括路由协议、DNS、SIP 和 SS7 等。

最终用户安全面涉及客户访问和使用服务提供者网络的安全。同时也考虑保护用户的数据流。最终用户使用网络可以只是提供连接,也可能用于诸如 VPNs 这类增值服务,也可能用来访问基于网络的应用。

5.4.2　安全体系结构参考模型的应用

参考体系结构能应用到安全程序的所有方面,安全程序包括策略、过程及技术。参考体系结构能指导综合安全策略、事故响应和恢复计划及技术体系结构的开发;在制定和规划阶段在每个安全层和安全面考虑每个安全维的控制措施。参考体系结构还能用作安全评估的基础,检验安全程序在制定策略和过程、开发技术时是怎样处理安全维、安全层和安全面的。参考体系结构有助于管理安全策略和过程、事故响应和恢复计划及技术体系结构,确保对安全程序的修改应满足在每个安全层和安全面上的安全维要求。

安全体系结构能应用到任何类型网络的协议栈的任何层。例如,在 IP 网络,位于协议栈的下三层,基础设施安全层包括各个路由器、在路由器之间的点到点通信(即 SONET、ATM 和 PVCs 等)及服务器平台用来提供 IP 网络需要的支持服务。服务安全层有基本的 IP 服务(即 Internet 连接)、IP 支持服务(即 AAA、DNS 和 DHCP 等)及由服务提供商提供的先进的增值服务(即 VoIP、QoS 和 VPN 等)。应用安全层是用户应用的安全,通过 IP 网络访问的用户应用安全(电子邮件等)。

可以根据参考体系结构划分成 9 个模块,每个模块包含应用到特定安全层和特定安全面的 8 个安全维。不同模块的各个安全维有不同的目标,因而由不同的安全方法组成。表 5-1～表 5-9 分别列出应用各安全维到不同的安全层和安全面。

表 5-1　应用安全维到基础设施安全层、管理安全面

模块 1:基础设施安全层、管理安全面	
安全维	安 全 目 标
访问控制	保证只有授权的人或设备允许实施或企图实施对网络设备或通信链路的管理活动。该应用适用于通过设备端口的直接管理或远程管理
身份鉴别	对网络设备或通信链路上实施管理任务的人或设备的身份进行验证。身份鉴别技术是访问控制需要的
不可否认	提供一个记录以认定在网络设备或通信链路上人或设备实施的每个管理活动。该记录能用来证明管理活动的源
数据保密	防止对网络设备和通信链路配置信息的非授权访问或观察,包括常驻在网络设备和通信链路的配置信息,正在传输到网络设备和通信链路的配置信息,以及离线存储的设备配置信息。防止对管理身份鉴别的信息(即管理者的身份和口令)的非授权访问或观察。用于访问控制的技术,也可用于数据保密

续表

模块 1：基础设施安全层、管理安全面	
安全维	安 全 目 标
通信流安全	对在网络设备或通信链路的远程管理，保证管理信息只在远程管理站和正在被管理的设备或通信链路之间流动，管理信息和在这些端点之间流的信息不被转移或拦截，包括应用的管理身份鉴别信息(即管理者的身份和口令)
数据完整性	防止网络设备和通信线路的配置信息非授权修改，包括常驻在网络设备或通信链路的配置信息，以及传输或存储在离线系统的配置信息，也包括管理身份鉴别的信息(即管理者的身份和口令)
可用性	保证授权的设备管理网络设备或通信链路的能力不能被拒绝，包括防止诸如拒绝服务这类主动攻击和诸如修改或删除管理身份鉴别信息这类被动攻击(即管理者的身份和口令)
隐私	保证能用来识别网络设备或通信链路的信息对非授权人或设备不可用，例如这类信息包括网络设备的 IP 地址或 DNS 域名，因为这些信息给攻击者提供了攻击目标信息。保证通过网络收集和处理个人信息应遵守本地数据保护法律、法规

表 5-2　应用安全维到基础设施安全层、控制安全面

模块 2：基础设施安全层、控制安全面	
安全维	安 全 目 标
访问控制	保证只有授权的人或设备允许访问或企图访问常驻在网络设备或离线存储的控制信息。保证网络设备只接受来自授权网络设备的控制信息报文
身份鉴别	对观察或修改网络设备上的控制信息的人或设备的身份进行验证。对发送控制信息到网络设备的设备身份进行验证。身份鉴别技术也是访问控制需要的
不可否认	提供一个记录以认定在网络设备上观察或修改控制信息的人或设备，该记录能用来证明控制信息的访问或修改。提供一个记录以认定设备将源控制报文送到网络设备，该记录能用来证明设备已发出了控制报文
数据保密	防止对常驻在网络设备或离线存储的控制信息的非授权访问或观察。用于访问控制的技术也可用于常驻在网络设备的控制信息的数据保密。防止正在网上传输的指向网络设备的控制信息的非授权使用和观察
通信流安全	保证正在网上传输的控制信息(即路由更新)只在控制信息源和目的站之间流动，在这些端点之间流动的控制信息不被转移或拦截
数据完整性	防止常驻在网络设备、在网上传输的、或存储在离线的控制信息非授权修改
可用性	保证网络设备总能从授权源接收控制信息，包括防止诸如 DoS 这类蓄意的攻击和偶然发生的(即路由摆动)
隐私	保证能用来识别网络设备或通信链路的信息对非授权人或设备不可用，这类信息包括网络设备的 IP 地址或 DNS 域名，因为这些信息给攻击者提供了攻击目标信息。保证通过网络收集和处理个人信息应遵守本地数据保密法律、法规

表 5-3　应用安全维到基础设施安全层、最终用户安全面

模块 3：基础设施安全层、最终用户安全面	
安全维	安 全 目 标
访问控制	保证只有授权的人或设备允许访问或企图访问在网络部件或通信链路正在传送的，或常驻在离线存储设备的最终用户数据
身份鉴别	对企图访问正在网络部件或通信链路传送的或常驻在离线存储设备的最终用户数据的人或设备的身份进行鉴别。身份鉴别技术也是访问控制需要的
不可否认	提供一个记录以认定传送在网络部件或通信链路或常驻在在线设备上的最终用户数据已被人或设备访问。该记录能用来证明最终用户的访问
数据保密	防止正在网络部件或通信链路上传输的或常驻在离线设备的最终用户数据的非授权访问或观察。用于访问控制的技术也可用于最终用户数据的数据保密
通信流安全	保证正在网络部件和通信链路传送的最终用户数据不被转移和拦截，也包括无授权访问的这些端点之间的数据流
数据完整性	防止正在网络部件或通信链路传输的，或常驻在离线设备的最终用户数据非授权修改
可用性	保证授权人(包括最终用户)和设备常驻在设备的最终用户数据的访问不被拒绝，包括防止诸如 DoS 这类主动攻击和诸如修改或删除身份鉴别信息(即用户身份和口令、管理者身份和口令)这类被动攻击
隐私	保证网络部件不提供有关最终用户的网络活动信息(用户地理信息、访问的 Web 站等)给非授权人或设备。保证通过网络收集和处理个人信息应遵守本地数据保护法律、法规

表 5-4　应用安全维到服务安全层、管理安全面

模块 4：服务安全层、管理安全面	
安全维	安 全 目 标
访问控制	保证只有授权的人或设备允许实施或企图实施网络服务的管理活动
身份鉴别	对网络设备或通信链路上实施管理任务的人或设备的身份进行验证。身份鉴别技术也是访问控制需要的
不可否认	提供一个记录以认定在网络设备或通信链路上的人或设备实施的每个管理活动，该记录能用来证明管理活动的源
数据保密	防止网络服务的配置和管理信息的非授权访问或观察，包括常驻在网络设备的管理和配置信息，正在网上传输或在线存储的管理和配置信息。防止网络服务的管理信息(即用户身份和口令、管理者的身份和口令)的非授权访问或观察
通信流安全	对网络服务的远程管理，保证管理信息只在远程管理站和正在作为网络服务一部分的管理设备之间流动，管理信息在这些端点之间的信息流不被转移或拦截，包括网络服务鉴别信息(即用户身份和口令、管理者身份和口令)
数据完整性	防止网络服务的管理信息非授权修改，包括常驻在网络设备、正在网上传输或离线系统存储的管理信息，也包括网络服务身份鉴别信息(即用户身份和口令、管理者身份和口令)

续表

模块 4：服务安全层、管理安全面	
安全维	安 全 目 标
可用性	保证授权人和设备管理网络服务的能力不被拒绝，包括防止诸如 DoS 这类主动攻击及诸如修改或删除服务管理身份鉴别信息(即管理者身份和口令)
隐私	保证能用来识别网络服务管理的信息对非授权人或设备不可用，例如，这类信息包括系统的 IP 地址或 DNS 域名，因为这些能识别网络服务管理系统的信息给攻击者提供了攻击目标信息。保证通过网络收集和处理个人信息在遵守本地的数据保护法律、法规

表 5-5　应用安全维到服务安全层、控制安全面

模块 5：服务安全层、控制安全面	
安全维	安 全 目 标
访问控制	保证网络设备接收到的控制信息来自授权源的网络服务。例如，防止来自非授权设备的欺骗的 VoIP 会话启动报文
身份鉴别	对参与网络服务的网络设备发送网络服务控制信息的源进行身份验证。身份鉴别技术也是访问控制需要的
不可否认	提供一个记录以认定对参与网络服务的网络设备接收到的网络服务控制报文发出的人或设备，该记录能用来证明人或设备已发出网络服务控制报文
数据保密	防止常驻在网络设备的网络服务控制信息(即 IPSec 会话数据库)，正在网上传输的或离线存储的网络服务控制信息的非授权访问或观察。用于访问控制的技术也可用于常驻在网络设备的网络服务控制信息的数据保密
通信流安全	保证正在网上传输的网络服务控制信息只在控制信息源和目的站之间流动。在这些端点之间的网络服务控制信息不被转移或拦截
数据完整性	防止常驻在网络设备、在网络上传输的或离线存储的服务控制信息非授权修改
可用性	保证参与网络服务的网络设备总能接收来自授权源的控制信息，包括防止诸如 DoS 这类主动攻击
隐私	保证能用来识别参与网络服务的网络设备或通信链路的信息对非授权人或设备不可用，这类信息包括网络设备的 IP 地址或 DNS 域名，因为这些信息给攻击者提供了攻击目标的信息。保证通过网络收集和处理个人信息应遵守本地数据保护法律、法规

表 5-6　应用安全维到服务安全层、最终用户安全面

模块 6：服务安全层、最终用户安全面	
安全维	安 全 目 标
访问控制	保证只有授权用户和设备允许访问或企图访问以及使用网络服务
身份鉴别	对企图访问和使用网络服务的用户或设备身份进行验证。身份鉴别技术也是访问控制需要的
不可否认	提供一个记录以认定每个用户或设备已访问和使用了网络服务，该记录能用来证明已被最终用户和设备访问和使用网络服务
数据保密	防止正在由网络服务传输的、处理的或存储的最终用户数据的非授权访问或观察。用于访问控制的技术也可用于最终用户数据的数据保密

续表

模块 6：服务安全层、最终用户安全面	
安全维	安 全 目 标
通信流安全	保证正在由网络服务传输的、处理的或存储的最终用户数据在无授权访问的这些端点(即合法的线抽头)之间的流动时不被转移或拦截
数据完整性	防止正在由网络服务传输的、处理的或存储的最终用户数据非授权修改
可用性	保证授权的最终用户或设备对网络服务的访问不被拒绝，包括防止诸如 DoS 这类主动攻击及诸如修改或删除最终用户身份鉴别信息(即用户身份和口令)这类被动攻击
隐私	保证网络服务不提供有关最终用户使用服务(即 VoIP 服务等)的信息给非授权人和设备。保证通过网络收集和处理个人信息应遵守本地数据保护法律、法规

表 5-7　应用安全维到应用安全层、管理安全面

模块 7：应用安全层、管理安全面	
安全维	安 全 目 标
访问控制	保证只有授权人和设备允许实施或企图实施基于网络应用的管理活动
身份鉴别	对企图实施基于网络应用的管理活动的人或设备身份进行验证。身份鉴别技术也是访问控制需要的
不可否认	提供一个记录以认定实施基于网络应用的每个管理活动的人或设备，该记录能用来证明用户或设备已经实施了管理活动
数据保密	防止用于生成和执行的基于网络应用的所有文件(即源文件、目标文件、可执行文件及临时文件等)以及应用配置文件的非授权访问或观察，包括常驻在网络设备的应用文件、正在网上传输的或离线存储的应用文件。防止基本于网络应用的管理信息(即用户身份和口令、管理者身份和口令)的非授权访问或观察
通信流安全	对基于网络应用的远程管理，保证管理信息只在远程管理站和包括在基于网络应用的设备之间流动，管理信息和这些端点之间的信息流不被转移或拦截，也包括基于网络应用的管理信息(即用户身份和口令、管理者身份和口令)
数据完整性	防止用于生成和执行的基于网络应用的所有文件(即源文件、目标文件、可执行文件及临时文件等)及应用配置文件的非授权访问，包括常驻在网络设备的应用文件，正在网上传输或离线存储的应用文件，也包括基于网络应用的管理信息(用户身份和口令、管理者身份和口令)
可用性	保证授权人和设备管理基于网络应用的能力不被拒绝，包括防止诸如 DoS 这类主动攻击及诸如修改或删除基于网络应用的管理身份鉴别信息(即管理者身份和口令)这类被动攻击
隐私	保证能用来识别基于网络应用的管理系统的信息对非授权人或设备不可用，这类信息包括系统的 IP 地址或 DNS 域名，因为能识别基于网络应用的管理系统的信息给攻击者提供了攻击目标信息。保证通过网上收集和处理信息应遵守本地数据保护法律、法规

表 5-8　应用安全维到应用安全层、控制安全面

模块 8：应用安全层、控制安全面	
安全维	安 全 目 标
访问控制	保证参与基于网络应用的网络设备接收到控制信息来自授权源。例如，防止来自非授权设备的欺骗的 SMTP 客户
身份鉴别	对参与基于网络应用的网络设备发送应用控制信息的源进行身份验证。身份鉴别技术也是访问控制需要的
不可否认	提供一个记录以认定对参与网络服务的网络设备接收到的网络服务控制报文发出的人或设备，该记录能用来证明人或设备已发出网络服务控制报文
数据保密	防止常驻在网络设备的应用控制信息(即 SSL 或 TSL 会话数据库)正在网上传输的或离线存储的应用控制信息的非授权访问或观察。用于访问控制的技术也可用于常驻在网络设备的、基于网络应用的控制信息的数据保密
通信流安全	保证正在网上传送应用控制信息(即 SSL 或 TSL 会话数据库)只在控制信息源和目的站之间流动，基于网络应用的控制信息及这些端点之间的信息流不被转移或拦截
数据完整性	防止常驻在网络设备的、在网上传输的或离线存储的基于网络应用控制信息的非授权修改
可用性	保证参与基于网络应用的网络设备总能接收来自授权源的控制信息，包括防止诸如 DoS 这类主动攻击
隐私	保证能用来识别参与基于网络应用的网络设备或通信链路的信息对非授权人或设备不可用，这类信息包括网络设备的 IP 地址或 DNS 域名，因为能识别网络设备或通信链路的信息给攻击者提供了攻击目标信息。保证通过网络收集和处理个人信息应遵守本地的数据保护法律、法规

表 5-9　应用安全维到应用安全层、最终用户安全面

模块 9：应用安全层、最终用户安全面	
安全维	安 全 目 标
访问控制	保证只有授权用户和设备允许访问或企图访问，以及使用基于网络的应用
身份鉴别	对企图访问和使用基于网络应用的用户或设备身份进行验证。身份鉴别技术也是访问控制需要的
不可否认	提供一个记录以认定每个用户或设备已访问和使用了基于网络的应用，该记录能用来证明最终用户或设备访问和使用了基于网络的应用
数据保密	防止正在由基于网络应用传输的、处理的或存储的最终用户数据(即用户信用卡号码)的非授权访问或观察，也包括从用户流向基于网络应用的用户数据。用于访问控制的技术也可用于最终用户数据的数据保密
通信流安全	保证正在由基于网络应用传输的、处理的或存储的最终用户数据不被转移或拦截，也包括无授权访问的这些端点之间的数据流
数据完整性	防止正在由基于网络应用传输的、处理的或存储的最终用户数据非授权修改，也包括从用户流向基于网络应用的用户数据
可用性	保证授权最终用户或设备对基于网络应用的访问不被拒绝，包括防止诸如 DoS 这类主动攻击及诸如修改或删除最终用户身份鉴别信息(即用户身份和口令)这类被动攻击
隐私	保证基于网络的应用不提供有关最终用户使用应用的信息(访问的 Web 站点)给非授权人或设备，这类信息只泄露给搜索证据的执法人员。保证通过网络收集和处理信息应遵守本地数据保护法律、法规

5.5 本章小结

可信系统体系结构要素包括定义主体和客体的子集、可信计算基、安全边界、基准监控器和安全内核、安全域、资源隔离、安全策略和最小特权等。

网络安全体系结构是一种层次安全结构,不同类型的漏洞、攻击和威胁存在于网络的不同层次,需要研究网络环境的各种技术,实施网络不同层次的保护。

开放系统互连安全体系结构(ISO 7498-2)是基于 OSI 参考模型的七层协议之上的信息安全体系结构。它定义了 5 类安全服务、8 种特定的安全机制、5 种普遍性安全机制。确定了安全服务与安全机制的关系,以及在 OSI 七层模型中安全服务的配置。它还确定了 OSI 安全体系的安全管理。

5 类安全服务是鉴别、访问控制、数据机密性、数据完整性及抗否认。8 种特定的安全机制是加密、数字签名、访问控制、数据完整性、鉴别交换、通信业务填充、路由选择控制及公证。5 种普遍性安全机制是可信功能度、安全标记、事件检测、安全审计跟踪及安全恢复。各项安全服务在 OSI 七层中都有适当的配置位置。

ISO/IEC 18028-2 定义了一个安全体系结构参考模型,它把一组复杂的端到端网络安全相关的特性逻辑上分解成各个结构组成,从而生成端到端的安全的有序方案,既可用于评估生成现有网络的安全,也可用于规划新的方案。安全体系结构参考模型有 3 个结构组件构成,即安全维、安全层和安全面。

习　题

1. 下面是几种对 TCB 的描述,正确的是(　)。
   A. 来自橘皮书,和固件有关
   B. 来自橘皮书,由操作系统实施的安全机制
   C. 来自橘皮书,是系统的保护机制
   D. 在安全环境中系统描述安全机制的级别
2. 下面(　)的存储提供最高安全。
   A. 内存映射　　B. 硬件分段　　C. 虚拟机　　D. 保护环
3. 基准监控器能确保(　)。
   A. 只有授权主体可访问客体
   B. 信息流从低安全级别到高安全级别
   C. CPU 不直接访问内存
   D. 主体不对较低级别的客体写操作
4. 保护域的正确定义是(　)。
   A. 可供主体使用的系统资源　　B. 在安全边界外的系统资源
   C. 在 TCB 内工作的系统资源　　D. 工作在保护环 1 到 3 的系统资源

5. 一种抽象机能保证所有主体有适当的允许权来访问客体，这种确保客体不被不可信主体损害的安全控制概念是(　)。

A. 安全核　　B. TCB　　C. 基准监控器　　D 安全域

6. CPU 和 OS 有多层自保护，它们用保护环机制通过安全控制边界把关键组件分开，下列(　)组件应放在最外环。

A. 应用和程序　　B. I/O 驱动器和公用程序

C. 操作系统 OS 核　　D. OS 的其余部分

7. TCB 内有几种类型的部件，下列(　)不在安全边界内。

A. 母板上的固件　　B. 应用程序

C. 保护的硬件组件　　D. 基准监控器和安全核

8. 处理器和系统运行在(　)状态能处理和硬件的直接通信。

A. 问题状态　　B. 等待状态　　C. 运行状态　　D. 特权状态

9. ISO 7498-2 从体系结构的观点描述了 5 种可选的安全服务，以下不属于这 5 种安全服务的是(　)。

A. 身份鉴别　　B. 数据报过滤　　C. 授权控制　　D. 数据完整性

10. ISO 7498-2 描述了 8 种特定的安全机制，这 8 种特定的安全机制是为 5 类特定的安全服务设置的，以下不属于这 8 种安全机制的是(　)。

A. 安全标记机制　B. 加密机制　　C. 数字签名机制　　D. 访问控制机制

11. 用于实现身份鉴别的安全机制是(　)。

A. 加密机制和数字签名机制

B. 加密机制和访问控制机制

C. 数字签名机制和路由控制机制

D. 访问控制机制和路由控制机制

12. ISO 7498-2 从体系结构的观点描述了 5 种普遍性的安全机制，这 5 种安全机制不包括(　)。

A. 可信功能　　B. 安全标号　　C. 事件检测　　D. 数据完整性机制

13. 身份鉴别是安全服务中的重要一环，以下关于身份鉴别的叙述不正确的是(　)。

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

14. 在 ISO/OSI 定义的安全体系结构中，没有规定(　)。

A. 对象认证服务　　B. 访问控制安全服务

C. 数据保密性安全服务　　D. 数据完整性安全服务

E. 数据可用性安全服务

15. (　)不属于 ISO/OSI 安全体系结构的安全机制。

A. 访业务流量分析机制　　B. 访问控制机制

C. 数字签名机制　　D. 审计机制

E. 公证机制

16. ISO 安全体系结构中的对象认证安全服务，使用(　)完成。

A. 加密机制　　B. 数字签名机制

C. 访问控制机制　　D. 数据完整性机制

17. CA 属于 ISO 安全体系结构中定义的(　)。

A. 认证交换机制　　B. 通信业务填充机制

C. 路由控制机制　　D. 公证机制

18. 数据保密性安全服务的基础是(　)。

A. 数据完整性机制　　B. 数字签名机制

C. 访问控制机制　　D. 加密机制

19. 路由控制机制用以防范(　)。

A. 路由器被攻击者破坏

B. 非法用户利用欺骗性的路由协议，篡改路由信息、窃取敏感数据

C. 在网络层进行分析，防止非法信息通过路由

D. 以上皆非

20. 数据完整性安全机制可与(　)使用相同的方法实现。

A. 加密机制　　B. 公证机制　　C. 数字签名机制　　D. 访问控制机制

21. 可以被数据完整性机制防止的攻击方式是(　)。

A. 假冒源地址或用户的地址欺骗攻击

B. 抵赖做过信息的递交行为

C. 数据中途被攻击者窃听获取

D. 数据在途中被攻击者篡改或破坏

22. 分组过滤型防火墙原理上是基于(　)进行分析的技术。

A. 物理层　　B. 数据链路层　　C. 网络层　　D. 应用层

23. 对动态网络地址转换 NAT，下面说法不正确的是(　)。

A. 将很多内部地址映射到单个真实地址

B. 外部网络地址和内部地址一对一的映射

C. 最多可有 64 000 个同时的动态 NAT 连接

D. 一个内部桌面系统最多可同时打开 32 个连接

24. ISO/IEC 网络安全体系结构的安全层提供网络安全的层次解决方案，下面说法不正确的是(　)。

A. 基础设施安全层支持服务安全层

B. 服务安全层支持应用安全层

C. 安全层的含义和 OSI 层次安全的含义是完全相同的

D. 应用安全层支持服务安全层

25. ISO/IEC 网络安全体系结构的安全维包含(　)个安全度量，用于实施网络安全的某一特定方面的安全控制措施。

A. 5　　B. 7　　C. 8　　D. 3

第 2 篇
Internet 安全体系结构

第6章 Internet 安全体系结构之一

本章要点:

- LAN 的攻击类型及防御方法;
- 无线网的风险及缓解方法;
- 数据链路层风险及缓解方法;
- PPP,MAC,ARP 的风险;
- 网络层风险及缓解方法;
- IP 风险及 IP 安全可选方案。

不同类型的漏洞、攻击和威胁存在于 Internet 的不同层次,Internet 安全体系结构就是依照层次结构的原则,对不同类型的攻击实施不同层的保护。本章重点分析物理层、数据链路层和网络层的风险以及缓解风险的方法,第7章分析传输层和应用层的风险以及缓解风险的方法。

6.1 物理网络风险及安全

6.1.1 物理网络风险

物理网的攻击集中在物理网部件。攻击包括窃听、回答(重放)、插入和拒绝服务(DoS)。这些攻击仅限于能物理访问的攻击者,限制物理访问也就限制了攻击的存在。

1. 窃听(eavesdropping)

物理连接器允许直接访问网络介质,这就使攻击者能窃听通过物理介质的数据。当网络有开放的分接头、可访问的分接头或物理访问介质,网络就易于被窃听。例如,攻击者能使用带开放端口的网络 hub 直接和网络接口并记录所有网络通信量。阻止或限制访问开放端口就能缓解风险。

可以将已有的结点从网络分接头断开,而插入一个敌意的结点;也可将网络分接头连到桥或分接器(spliter),为敌意的结点生成一个开放分接头。对物理电缆,网络链路可被切断,插入一个连接器,以允许网络被窃听。一些灵敏的连接器可检测到电缆上的信号,并传送到另一个电缆;类似的原理,使用高灵敏度的接收器来侦察从监控器、计算机芯片或网络电缆发射的 RF 辐射,而无线网络更易于广播侦察。

2. 回答(重放)

窃听是一种相对被动的攻击,能经常进行而不被检测。另一种是主动攻击,因为网络连接器允许发送,也可接收,攻击者能主动发送数据到网上。回答攻击是基于记录网上接收到的信号,并给网络返回。这种类型攻击,不需要知道数据的意思,而仅仅是将其返回。

3. 插入

类似于回答攻击,插入攻击是发送数据,但不是返回接收到的数据,而是新的数据。这种攻击通常是用来访问目标系统的网络高层。例如,假如网络基于物理层身份鉴别限制访问,攻击者可窃听网络,并在身份鉴别完成后插入数据。

4. 拒绝服务(DoS)

物理网络是最易受 DoS 攻击的,包括不经意的和故意的。不经意的 DoS 诸如 hub 的电源接插头掉了,网络连接器碰掉了等。故意的 DoS 攻击包括物理切断电缆,或将低压电缆插入高压源,以致将网络设备烧断等。对 RF 电源和无线网络,无线频率干扰 RFI 是最有效的破坏网络的方法,包括不经意的和故意的。

6.1.2 物理层安全

物理层提供对物理链路的访问,以及对通过物理介质传输的数据编码和解码,没有通用的物理层协议直接提供安全。身份鉴别、授权、验证是由高层协议来管理,一般是由数据链路、网络或会话层来管理。

很多物理层协议的身份鉴别是和高层紧密相连的,例如拨号网和无线网。拨号网通常是依靠 PPP 或 SLIP 来进行用户身份鉴别的,而无线网对客户的身份鉴别是使用 WEP 协议(Wired Equivalent Privacy)和 MAC 地址过滤进行的。

多数情况下,物理层是作为身份鉴别栈的一部分来实现的。身份鉴别栈是一个 OSI 栈,它位于网络用户的 OSI 栈的前面,管理网络的身份鉴别。当数据到达结点时,身份鉴别栈处理数据并验证信息,身份鉴别信息再送到结点的 OSI 栈,如图 6-1 所示。

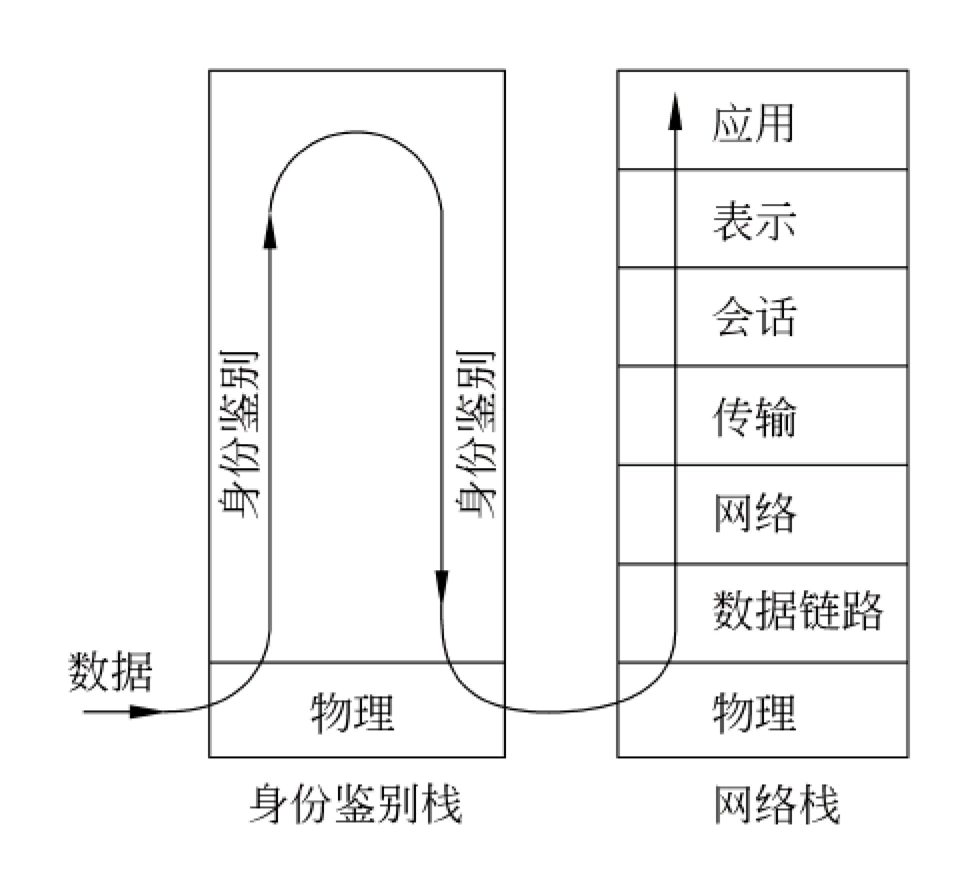


图 6-1 一个简单的网络身份鉴别栈

对物理层攻击源的识别能力取决于网络介质、配置和规模。总线网络比星型网络更难识别,对网线的破坏和无线电频率干扰 RFI 的识别则更加困难。对大规模网的攻击识

别比小规模网又要困难得多。

6.2　局域网 LAN 的安全

6.2.1　攻击类型

对有线物理网的攻击包括连接破坏、干扰、侦察和插入攻击。

1. 破坏(disruption)

对物理网连接的破坏包括中断电源和切断网络电缆。缓解的方法包括配置备用电源和限制访问核心网络设备。

2. 干扰(interference)

物理介质用来传送数据和其他信号。假如非授权的信号(如干扰)进入介质,则网络设备可能无法区别数据和噪声。因此,大部分物理层协议明确地说明介质的屏蔽要求以阻止周围的噪声进入网络。另外采用数据编码技术也可缓解对干扰的影响。虽然大部分网络规范定义对干扰有一定的容忍度,但是强的无线电频率干扰靠近网络电缆仍能使网络无法正常传输数据。

3. 故意攻击(intentional attacks)

来自侦察、回答和插入攻击的威胁通常是故意的。可以通过网络配置来缓解这些威胁。可选的方案包括防火墙以及提供 DMZ 等定位的网络配置。

6.2.2　防御方法

防御方法有以下几种:

1. 防火墙

最有效的方法是将网段分隔开来,直接连到 Internet 的系统是没有任何保护的。防火墙是在网段之间过滤网络通信的系统以及能保护特定的网络的协议。防火墙基本上是和协议低层相联系的,包括物理层、数据链路层、网络层和传输层。缓解方法的选择是基于防火墙能实现的网络通信过滤。

防火墙至少将网络分成两个网段,一段是可信的 LAN,另一段是不可信的 WAN。防火墙的实施可分软件防火墙和硬件防火墙两大类,也有专门为家庭用户的防火墙。它们在价格、复杂性、灵活性、个人化和过滤能力方面有很大区别。

2. 特权区(privileged zones)

单个防火墙能在不太可信的 WAN 和更可信的 LAN 间生成一个壁垒,单个防火墙定义两个特权区。在一个组织内,往往有不同程序的可信度,可以使用分段拓扑,在物理层明确地定义。分段的拓扑可以是不同可信级别的分段串联起来,但更为普遍的是采用 DMZ、洋葱头拓扑和大蒜头拓扑,如图 6-2 所示。

DMZ 是在 LAN 和 WAN 之间的一个隔离的网段。虽然在 DMZ 和 LAN 之间存在物理连接，但真正的连接是依赖诸如路由器和网关这类网络设备，在网络高层完成连接。DMZ 对网络安全提供 3 个关键的好处：限制数据流、限制物理连接以及监控访问点。

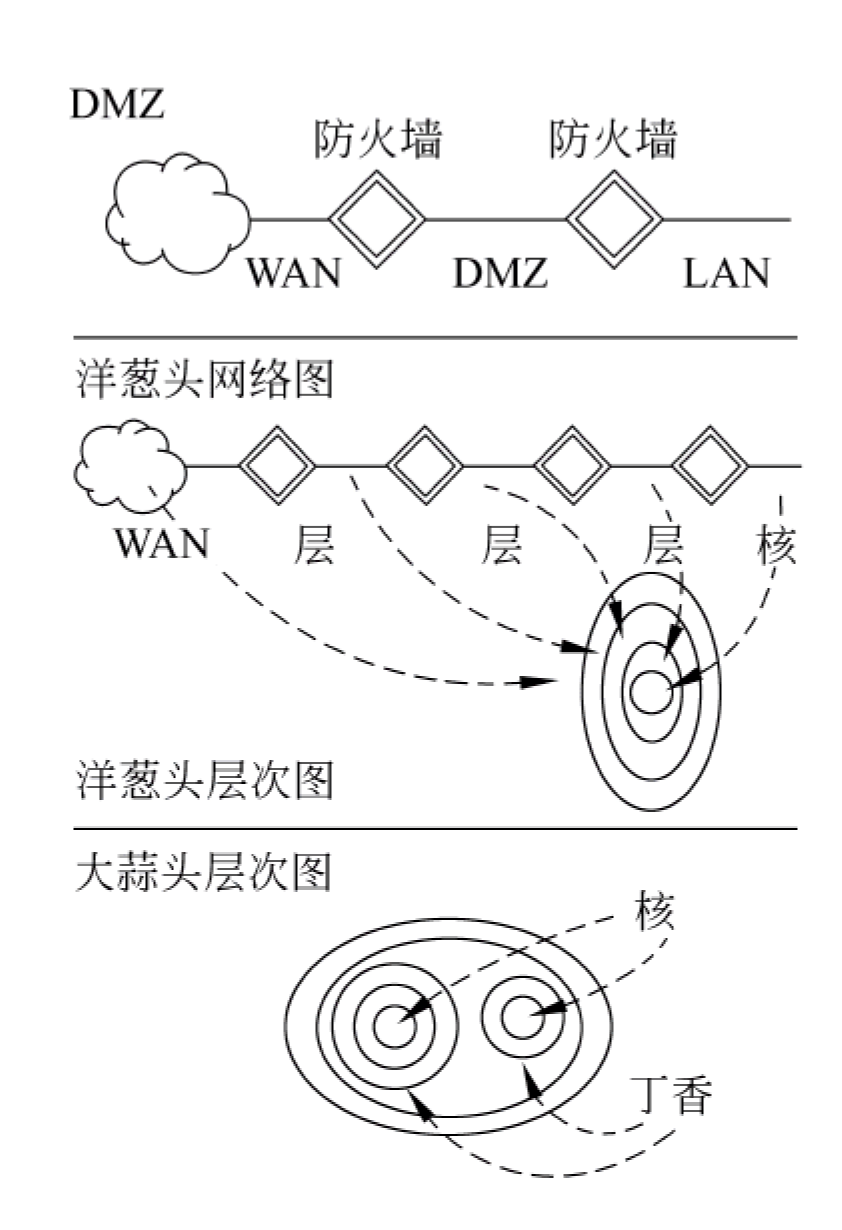


图 6-2　DMZ、洋葱头、大蒜头网络配置

洋葱头网是由防火墙将众多 LAN 分隔成串联层。每层叫作一个环，对邻近的环是独立的网段。洋葱头的中心层称为核，每个洋葱头只包含一个核。层间的防火墙限制访问每层，对核心层更是有严格的限制。

分层的网络簇(cluster)形成大蒜头网，也称气泡网或单元网。每个大蒜头网称一个丁香(clove)，每个 clove 包含一个核。不同的 clove 可以有不同的深度，也可以包括含有附加 clove 的子网。大蒜头网的主要安全特点是它的组织结构，每层(或核)的结点不能和不同层的结点进行通信，除非经过一个网络通路通信。

3. LAN 连接

为了利用物理层的安全风险，攻击者必须连到 LAN。LAN 通常是动态的，系统周期地出现和消失，但是物理网的连接可以是静态的，也可以是动态的。

静态连接是结点和网络之间有一条物理链路。即使结点不在线，但链路总是存在。攻击者有很多选择来利用静态连接，因为它是到物理网络的直接链路，风险包括开放的分接头、分接头拦截、拼接处及勾引针(vampire clips)。

动态网络链路是网络连接时，物理链路是变化的。拨号 modem 池是动态网络链路的典型例子，modem 服务器和 modem 客户端之间的物理通路在每次呼叫时是变化的。呼叫序列可以来自不同计算机，以及经过电话系统采取不同路由。因为通路是动态的，窃听客户端或服务器的电话链路，识别网络路由、窃听客户端或服务器的电话链路的任意点都是困难的。动态网络链接的时间也是不同的，一般用电话 modem 有可能几小时，但用电缆 modem 有可能持续很长时间。

电话 modem 连接同电缆 modem 网有类似的功能及风险。两者都是在不同的介质上通过网络通信，都允许双向网络连接，都从防火墙得到相同的好处。但两者在速度和访问方面都有显著的区别。

电话 modem 比电缆 modem 的传输速度要低很多，对于 DoS 攻击来说，较低速率的网络连接更易受攻击。例如，每秒能产生 20 个 ICMP ping 分组的攻击对电缆 modem 不会产生明显的延迟，而对 56Kbps 的电话 modem，这种 DoS 攻击就会产生明显的效果。

电缆 modem 很少连接到公司的 LAN，用户是通过 WAN 连接到 Internet 来访问服务。电话 modem 经常是直接连到 modem 池，并提供直接的 LAN 访问。如果攻击者知

道 modem 池的电话号码，就可用电话 modem 直接攻击公司 LAN。

为此，电话 modem 提供身份鉴别的可选择方案，以限制从动态 modem 连接进行物理层访问。每个 modem 服务器包括一个类似防火墙的网络栈，将 modem 和 LAN 隔开来，在取得访问以前提供一个身份鉴别点。

身份鉴别的可选方案有 modem 身份鉴别凭证、呼叫者 ID、自动回叫及生成安全动态链接等。

- modem 身份鉴别凭证：很多 modem 池要求登录凭证，如用户名和口令。第二层协议，诸如 PPP 和 SLIP 能请求和鉴别登录凭证。但用户名和口令有很多方法可破解，包括口令猜测、口令破解、拨号窃听等，变更的方法是用智能令牌的身份鉴别，这种密码系统产生动态值，以确保每次有不同的身份鉴别证书。口令和智能令牌也可用于网络更高层的身份鉴别连接。对于大部分基于凭证的系统身份鉴别只是发生在连接的初始阶段，在链路建立以后就没有身份鉴别，因此，对物理层的窃听和拦截仍然是可能的。
- 呼叫者 ID：呼叫者 ID 系统是基于呼叫方的电话号码对呼叫者进行身份鉴别。当呼叫电话时，本地电话交换发送一个自动号码识别 ANI(automatic number identification)码。接收电话方将收到的码作为呼叫 ID 的身份鉴别。但是呼叫 ID 不总是正确的，因为呼叫 ID 码在使用 ISDN、PBX 或 VoIP 系统时可以是假的。如采用操作员帮助呼叫，操作员可用手动方式输入一个码 ONI(operator number identification)，即审慎地提供一个变换的呼叫 ID 值。
- 自动回叫：很多安全系统采用自动回叫，即 modem 池呼叫客户，而不是回答电话。为了启动一次电话呼叫，呼叫者拨一个预先确定的电话号码。接收系统回答呼叫(或只是记录这个电话响)，可以使用呼叫 ID 或其他凭证对呼叫者进行身份鉴别。随后 modem 池呼叫回客户，回叫可以是对呼叫者 ID 或一个静态号码。客户回答该回叫，并完成任何其余的身份鉴别步骤。这样一个复杂的握手过程，可以使对外的呼叫无法通过呼叫者 ID 伪装来拦截。
- 生成安全动态链接：一个十分安全的拨号系统使用两个或更多的身份鉴别机制，包括口令、智能卡、呼叫者 ID、自动回叫以及基于其他凭证的验证。这种深度防御可限制单个危害的影响。

6.3 无线网络安全

6.3.1 无线网风险

无线网面临着一系列有线网没有的不安全风险，包括分组嗅测、SSID 信息、假冒、寄生和直接安全漏洞。

1. 分组嗅测(packet sniffing)

这是无线网络攻击的最简单方式。在无线网上的数据流本质上是一总线结构。每个

用户点 SP(subscriber point)接收到从访问点 AP(access point)发送的全部数据,这意味着接到 AP 的任何 SP 能观察到至少一半的客户的网络通信(经常是全部通信)。这直接导致会话拦截或对网络其他层的攻击。

2. 服务集标识 SSID(the service set identifier)信息

SSID 通常设置为一个公司名、家庭名或街道地址。这种数据类型能被潜在的攻击者破坏。SSID 中的值对用户有帮助,但同样也为攻击者所利用。

3. 假冒(impersonation)

AP 假冒可能是故意的,也可能是不经意的。攻击者可以在已有的 AP 附近建立一个新的 AP,并且赋以同样的 SSID。对存在多个 AP 的场合,SP 如何区别真实的 AP 和假的 AP 呢? 从 SPs 的观点,所有相同 SSID 的 AP 看起来是一样的。

由 IEEE 802.11 定义的有线等效隐私 WEP(wised equivalent privacy)协议对区别真实的和假冒的 AP 可能是有用的。但攻击者可以破坏 WEP,决定 WEP 的密钥,并赋予假冒的 AP。在抓到了一个不知觉的被骗者后,假冒者可做很多事情,包括拒绝服务 DoS;MitM(man-in-the-middle)攻击,即在途中拦截或修改被骗者打算使用的数据;隧道攻击,即攻击者在假冒的 AP 和真实的 AP 之间生成一个隧道,被骗者无法识别这类 MitM 攻击。

不经意的假冒发生在住户邻居可能对 AP 使用相同的设置,这种设置经常是默认的。

4. 寄生者(parasites)

寄生者要通过一个开放的 AP 来访问 Internet。假如一个无线网是开放的(没有 WEP),寄生者可以连接到 Web 进行浏览或收发 E-mail。大部分寄生者可被 WEP 检测到。

5. 直接安全漏洞(direct security breaches)

无线网络允许直接访问到物理网络,而 WEP 对决意的攻击者无法制止。

6.3.2　风险缓解的方法

如同有线网一样,无线网的介质并不提供安全机制。任何攻击者能拦截无线信号,立即访问物理网。为了缓解这种风险有 3 种可选方法。第 1 种选择是减少无线网的吸引力,这是技术上的模糊安全。对 SSID 打标签,不使 SSID 广播以及选择天线的位置都是深度防御的组成。第 2 种选择是限制攻击者连接和使用无线路由器的能力,MAC 过滤、WEP 以及其他密码系统对身份鉴别栈确定不同的阶段。最后一种是网络体系结构能限制成功攻击者的影响。

1. SSID 打标签

SSID 的设置值可以给攻击者提供信息,一个攻击者更有可能攻击一个已知的网络。最好的情况是 SSID 对拥有者应提供清楚的信息,而对攻击者是模糊的。例如,“CSL3-5”是指在 5 号楼的计算机安全实验室的 3 号路由器。

2. 广播 SSID

路由器每隔几秒钟广播 SSID，可使寻找 AP 的用户能发现它。可以不经常广播，而用户在需要连接前知道 SSID 的名字。虽然不能使所有不同的 SSID 广播机制不起作用，但可以大大减少受攻击的风险。

3. 天线放置

天线的位置直接影响接收信号强度。把天线放在地下室的墙角，就可限制接收的范围，还可采取一些措施，以限制信号在特定方向的传播。即使这样，仍不可能阻止决意的攻击者。方向性天线能提高 SPs 接到 AP 的能力，以访问十分远和十分弱的信号。

4. MAC 过滤

身份鉴别栈可严格地限制那些能收到无线信号的攻击者的访问。最简单的身份鉴别是基于网络协议第 2 层，即介质访问控制 MAC，MAC 地址能唯一识别每个网卡。很多 APs 允许管理者清楚地列出连接到路由器的 MAC 地址，这可阻止想连接到未知 MAC 地址的攻击者。但是大部分网卡允许用户改变 MAC 地址，因为 MAC 在每个分组中发送，一个攻击者仅需接收一个分组来识别一个有效 MAC 地址。

5. WEP

一个熟练的攻击者能很容易旁路 SSID 的设置、天线的设置，以及 MAC 过滤等防御措施，因为这些方法只是限制攻击发现，但不能阻止无线连接。相反，WEP 能主动阻止连接，即使仅仅是几分钟时间。虽然 WEP 不是主要用于技术攻击者，但确实对开放网络的安全是一个更好的选择。尤其是从法律的观点看，WEP 有一个重要的目的，即 WEP 可确定意图，一个攻击者解密和访问一个有 WEP 的网络，就很清楚地暴露其有意攻击的意图。

WEP 是通用的，已被大家所接受。几乎所有无线网络路由器都支持 WEP，并且相互兼容，这种普遍的接受导致很高的采用可能性。

6. 其他密码系统

WEP 不是唯一可用的密码系统。例如，IEEE 802.11i 定义了一个支持身份鉴别协议的方法，叫做 Wi-Fi 防护访问 WPA。身份鉴别系统有基于临时密钥完整协议 TKTP（Temporal Key Integrity Protocol），是针对静态 WEP 密钥的；有扩展身份鉴别协议 EAP（Extensible Authentication Protocol），是为阻止 MitM 攻击而设计的。

此外还有很多不限于开放标准的身份鉴别协议，虽然不同于 WEP 的协议提供了足够的安全以限制非授权的连接，但是都有两个主要的缺点：兼容性和可辨别性。前者导致不同厂商的硬件和驱动器不能相互兼容，一个厂商提供的身份鉴别栈不能支持和兼容其他厂商。后者是这些安全方法虽然能阻止攻击，但并不能阻止攻击者观察到网络。通过监控网络通信量，攻击者可知道网络的使用状况和网络数据流向等。

7. 网络体系结构

无线网允许任何人在接收范围内访问物理介质。身份鉴别栈可以阻止攻击者连到无

线网,而恰当的网络结构可对已经成功连接到无线路由器的攻击者限制其影响。诸如 DMZ 或 VPN 都是可选方案。

DMZ 将无线系统和 LAN 的其余部分分隔开来,连接到 AP 的任何 SP 只能访问 DMZ,进一步访问需要具有身份鉴别的能力,或旁路 DMZ 防火墙。

VPN 使主机和子网间的网络通信通过隧道进行,以确保在通过公共通道时的隐私。VPN 的解决方案很多,诸如安全壳 SSH(secure shell)、基于安全套接字层 SSL(secure socket layer)的开放网络、CIPE、PPTP、VTun(virtual tunnel)等。不同的 VPN 解决方案在安全和网络性能方面有不同的折中。理想的结构是使用洋葱头或大蒜头的配置,AP 放在中心核,攻击者即使能连接到 AP,但由于防火墙而不能访问 LAN 和 WAN,相反授权的用户能访问 LAN 并执行各个作业。

6.4 数据链路层风险及安全

6.4.1 数据链路层风险

数据链路层通常提供到物理层的接口,以确保数据在网络两个结点之间安全传递。然而,对一些不正常的使用表明网络受到攻击,这些攻击包括随意模式的监控、网络负载、寻址、在帧外的(out of frame)数据以及数据通道。

虽然有很多类型的不正常使用和滥用,但它们都需要直接物理访问到网络。这些攻击的范围仅限于数据链路层。对连接到路由器和网关的网络,这些滥用能给予防护。

1. 随意模式

在正常模式下,网络寻址机制(也就是 MAC)能阻止上面的堆栈层接收非指向该结点的数据。然而很多网络接口支持无地址过滤,运行在随意模式的结点能接收所有报文帧,而不只是指向该结点的帧。随意模式允许攻击者接收所有来自网络的数据。

- 随意模式攻击:随意模式通常用于网络分析和查错工具,网络管理者利用这种模式可以观察所有本地网络通信。然而,攻击者也能使用这个工具。攻击者可以看到明文传送的数据;可以看到在网上的系统数量和类型、通信类型以及网络活动时间;知道了网上数据的类型,攻击者即可接管已建立的连接;通过监控网络通信,攻击者可得到预警信号,它的存在已被检测到。
- 常用工具:有很多工具可将网络接口转到随意模式,这些工具包括 Tcpdump 一个在随意模式下捕捉网络分组的一个简单工具;Snort 一个功能很强的分组捕获工具,可用于 IDS,IPS 等应用;Ngrep 允许对特定的字节序列的网络通信进行扫描;Ethereal 捕获分组,重组通信,辨认大部分第 2 层协议。
- 检测随意模式:随意模式能旁路掉第 1、2 层的过滤,所有接收到的数据被送到网络层及其高层处理。但随意模式有一个最大的局限性,即很多高层协议假设网络数据在低层已被检测到。假如在分组内的数据要求做出回答,高层协议可以回答:例如 ARP,ICMP 和 DNS。

- 使用 ARP 检测连接随意模式：每个 ARP 分组包含一个硬件地址和一个 IP 地址。正常模式下，接收结点首先检查硬件地址，假如地址指标是该结点，则 ARP 的 IP 地址队列被处理。假如硬件地址和主机不匹配，则数据链路层拒绝该分组。然而在随意模式下分组被接收，并产生一个 ARP 回答响应。因此，随意模式能远程检测到，只要发送一个带有无效硬件地址、有效 IP 地址的 ARP 分组，送到每个结点。为了检测随意模式，不同的系统需要不同的 ARP 分组，因为随意模式的处理是基于兼容的硬件、驱动器的操作系统的组合。
- 使用 ICMP 检测随意模式：ICMP 回答分组(如 ping 分组)通常是从活动主机产生一个 ICMP 回答。多个 ICMP 分组应该产生多个具有相似延迟的回答。在随意模式下，结点接收更多分组要处理，因此有更大的延迟。
- 使用 DNS 检测随意模式：很多分组捕获工具，根据捕获到的 IP 地址查找主机名。检控 DNS 请求能决定哪个主机正在执行很多主机名的查找。

2. 负载攻击

数据链路层基本上是一个软件层，这意味着需要处理器来处理每个分组。大部分数据链路地址过滤只需十分低的开销，而高层经常需要消耗更多 CPU 资源。数据链路攻击会明显增加结点的 CPU 负载。

在多主机的网络，每个主机接收每个广播帧，这些帧必须通过数据链路层，在该层以及高层进行处理。简单的接收处理和处理单个广播报文帧，不会消耗很多资源。但是上千个广播分组的处理，对结点产生很多开销，对实时或关键服务器产生严重影响。

3. 地址攻击

大部分地址机制允许一个结点改变有效网络地址。假如两个结点配置成相同地址，其结果是两者都被拒绝网络连接。

使用网络地址作为访问标记的系统很容易被摧垮。攻击者正是需要将地址改变为任何允许值，在随意模式下观察网络，攻击者能识别可接受的地址。

4. 帧外数据

对不包含在报文帧内的数据通常会被丢弃。然而不包含在报文帧的信息能在物理层传输。这个帧外数据能节省网络带宽，或将信息转换成非标准形式。

运行在随意模式的网络接口可以接收帧外数据，但是这种能力依赖于物理层和数据链路层之间的接口。假如 100Base-T 以太网网卡可获取帧内和帧外数据，但无线网卡通常将帧外数据作为噪声丢弃掉。

5. 转换通道

数据链路层除了成帧和传播数据以外还可以有别的用处。很多高层功能可在数据链路层执行。攻击者能生成后门和类似数据链路层协议的远程控制协议。例如，信息能隐藏在标准报文帧以外，而大部分结点将忽略这些数据；当目的地址不是该结点，结点会忽略该帧，无效地址信息通常不检测；无效帧通常要丢弃，转换通道可以不经意地生成带有无效检查和的帧；网络支持可变帧长，可用来通过敏感信息，且难以检测；很多标准协议可

采用非标准方式来隐藏和传输信息，例如，ARP 在 ATM 网能很容易在以太网或其他非 ATM 网工作，这些分组是有效的，能通过网桥，但通常是不能检测的。数据链路通道通常限于本地网使用。

6. 物理风险

理论上讲，数据链路层是独立于物理层运行的，物理层能被替换而不影响数据链路层，例如，将 10Base-T 换成 100Base-T 无须改变数据链路层。因为这种独立性，数据链路层对所有物理层风险易受攻击。例如，物理层攻击者能直接访问数据链路报文帧；物理层攻击者能窃听所有数据链路通信；物理层攻击者能记录和回答数据链路通信，而且回答数据能被数据链路层接收；物理层攻击者能使用插入攻击生成一个带有有效数据链路报文帧的负载攻击。

6.4.2　数据链路层风险缓解方法

有若干种缓解数据链路风险的方法，包括硬编码硬件地址、数据链路和高层身份鉴别机制以及一些分析器和工具。

1. 硬编码

虽然对点到点网络的拦截风险是很低的，但对多结点网络数据链路地址系统的攻击是易于损坏的。攻击者能拦截和重指硬件地址。为了缓解这个问题，地址表可设置成静态地址。虽然对大的动态网络这种方法未必是可行的，但静态地址表对攻击者企图攻击动态地址表确实可提供一种防护。

静态地址表对改变已建立的系统进行防护，并阻止非授权的连接。例如，一个拨号服务器可存储一张可接受的呼叫者 ID 值的表，呼叫者如果提供不同的呼叫者 ID 值就会被拒绝。又如，很多无线网络限制客户只使用允许的无线 MAC 地址访问。

2. 数据链路身份鉴别

少数数据链路层协议实施加密，数据链路协议加密的处理开销是很昂贵的，对繁忙的网络易受负载攻击。代替的办法，有两种主要的密码解决方法，由 RFC 1334 定义的 CHAP 和 PAP，这些方法最初是用于点对点连接。

挑战握手身份鉴别协议 CHAP（The Challenge-Handshake Authentication Protocol）使用共享密钥对初始网络连接进行身份鉴别。CHAP 提供了一种方法对两个结点进行身份鉴别，但是在连接建立后不执行任何验证或加密。

口令身份鉴别协议 PAP（The Password Authentication Protocol）比 CHAP 要简单得多，登录凭证（id 和口令）用明文从客户传送到服务器。假如服务器接收凭证，则允许连接。PAP 没有加密，对拦截或回答攻击没有保护。

3. 高层身份鉴别

保护数据链路层最普遍的方法是依靠高层协议。假设任何身份鉴别、验证、密码系统将运行在高层以防止拦截、回答以及其他网络攻击。但是这种假设通常是不正确的。高层协议有可能不提供安全机制，有可能提供弱的安全方案。只有少数高层协议对数据链

路层进行身份鉴别。

4. 分析器和工具

诸如 IDS 和 IPS 这些网络应用软件依靠随意模式下监控网络的能力。诸如 Tcpdump，Snort 和 Ethereal 这类工具容易收集、识别和分析非预期的网络通信。

6.5 PPP 和 SLIP 的风险

PPP 和 SLIP 最大的风险是身份鉴别，双向通信和用户教育。虽然窃听、回答以及插入攻击是可能的，但这些攻击需要访问物理层。因为点到点网络只有两个结点在网上，物理层的威胁对数据链路层通常不是主要的考虑因素。

1. 身份鉴别

SLIP 不提供身份鉴别机制，而 PPP 支持 PAP 和 CHAP 身份鉴别。PAP 使用一个简单的凭证系统，包含用户名和口令，送到服务器的用户名和口令不加密，然后对已知的凭证进行验证。

CHAP 使用一个更复杂的系统，它是基于密钥交换和共享密钥，如图 6-3 所示。它不是直接发送凭证，CHAP 从客户端发送一个用户名到服务器（即身份鉴别器），服务器用一个 8 位的 ID 和一个可变长的随机数回答。ID 用来匹配挑战响应，以保持 CHAP 会话。客户返回一个 ID、共享密钥和随机数的 MD5 哈希函数。服务器计算自己的哈希函数并和客户的哈希函数进行比较。如果两者匹配，则表示有相同的共享密钥。

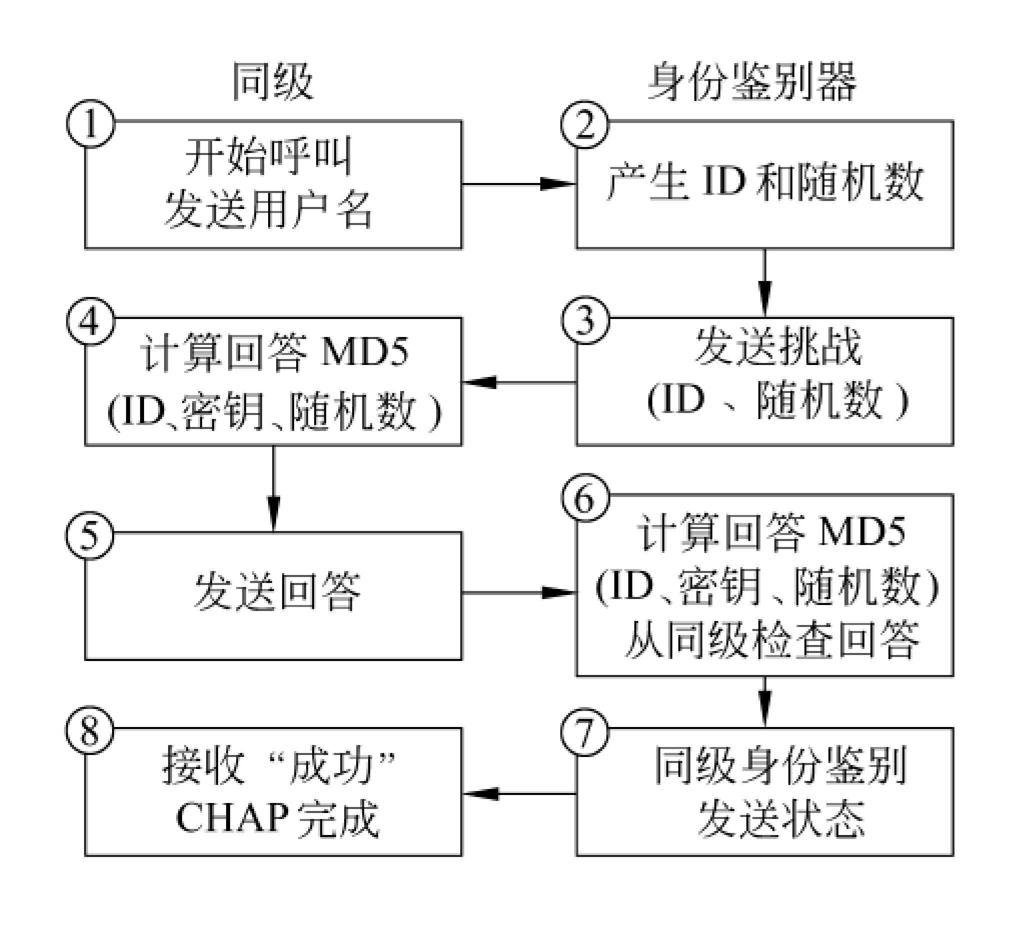


图 6-3　CHAP 处理

CHAP 的身份鉴别相当安全，可用于易受窃听攻击的网络。然而，CHAP 有两个局限性，首先，它只是在启动连接时进行身份鉴别，之后 PPP 不提供安全，某些攻击者具有在身份鉴别后拦截连接进行窃听的能力。其次，假如窃听者捕获到两个不长的随机数的协商，那么，对蛮力攻击，哈希函数可能易受攻击。

对 PAP 和 CHAP，服务器都必须保存带有全部凭证信息的文件。但它们都不支持

强的身份鉴别方法,传输的数据又没有加密,因此,窃听者能看到登录凭证。

2. 双向通信

PPP 和 SLIP 提供全数据链路支持,结点可和远程网络通信。远程网络也可和该结点通信。也就是 PPP 和 SLIP 提供全双向通信支持。因此,任何运行在远程客户的网络服务可被整个网络访问。大部分拨号用户并不使用防火墙,因此,开放网络服务系统易于受攻击。

软件防火墙或家庭拨号防火墙提供缓解方法,以减缓开放网络服务的风险。

3. 用户教育

大部分拨号、DSL 和电缆 modem 用户并未意识到他们的连接是双向的。更糟的是有些防火墙和在线游戏、会议系统软件是冲突的。这样,即使有防火墙,仍然有风险。

对高速拨号连接诸如 DSL 和 ATM 使用点到点物理连接,DSL 使用 PPPoE(PPP over Ethernet),ATM 使用 PPPoA(PPP over ATM)。对这些配置,数据链路层提供虚拟的透明连接。物理层访问的攻击者并不会被任何数据链路安全措施所阻止。

6.6　MAC 和 ARP 的风险

6.6.1　MAC 的风险

虽然 MAC 对网上的主机间提供了信息通信的方法,但是它也引入了潜在的攻击因素。攻击者可以利用 MAC 信息来侦察、伪装和基于负载的直接攻击。

1. 硬件框架(profiling)攻击

攻击的第一步是侦察。攻击者盲目地企图攻击一个未知系统是很少会成功的。组织的唯一标识 OUI(organizationally,unique identifies)对攻击者提供了硬件和操作系统的信息,例如,攻击者发现带有 OUI 为 00:0D:93 的源 MAC 地址,就可知是 Apple 计算机,操作系统是 Mac OS;OUI 为 00:20:F2 表示运行 Sun OS 或 Solaris 的 Sun Microsystems 计算机。

对数据链路层的攻击需要直接物理层访问。虽然硬件框架是可行的信息侦察技术,但攻击者需要已知系统的类型。为了模糊硬件框架,大多数网络驱动器允许改变 MAC 地址。改变 MAC 地址的方法,对不同操作系统是不同的,而某些驱动器并不支持。

2. 伪装攻击

具有管理特权的用户能改变 MAC 地址。攻击者可以故意改变地址,并复制到网上另一结点。假如这两个系统同时在网上活动,两者会互相干扰,这就成为有效的 DoS 攻击。

在某种情况下,两个相同硬件地址的结点能在网上共存。假如两者使用不同的网络层服务,或不同的数据链路服务访问点 SAPs,就可没有干扰地同时运行。这种类型的伪装可以旁路某些 IDSs,特别是对基于硬件地址过滤的特定结点。

3. 负载攻击

作为 OUI 的组成部分，第一个八位包含地址标志，其中最低位指示多播分组，奇数值是多播，FF 是指广播分组。攻击者能很快发起一个负载攻击，因为它能将地址改变为多播或广播地址。虽然这对攻击者的系统没有影响，但网上其他结点将处理攻击者发来的每个分组。

6.6.2 ARP 和 RARP 的风险

ARP（The Address Resolution Protocol）将 IP 地址转换成硬件地址，而 RARP（The Reverse Address Resolution Protocol）则将硬件地址转换成 IP 地址。ARP 和 RARP 请求是广播分组，并含有询问信息。例如，ARP 请求包含一个 IP 地址，所有在网上的结点接收到广播信息，但只有一个结点确认该 IP 地址，并发送一个回答报文给询问主机。查询结果存在一张 ARP 表，ARP 表列出所有在局域网上响应 ARP 请求的结点。

1. ARP 损坏（Poisoning）

映射 IP 地址到硬件地址或反之，对网络连接会产生一个延迟。ARP 表包含一个临时的缓存，以存储最近看到的 MAC 地址。因此，只有一个新的 IP 地址（或 MAC 地址）要查找时，才需要 ARP 分组。但是当一个无效的或不经意的差错进入 ARP 表，这个缓冲就会使系统的 ARP 受损。

2. ARP 受损的影响

ARP 受损的影响包括资源攻击、DoS 攻击和 MitM 攻击。

（1）资源攻击

一些系统能缓冲 ARP 条目的数是有限的，当大量假的 ARP 条目发送，ARP 表会填满。当填满后，有两种处理选择：忽略新的 ARP 或丢掉老的 ARP 条目。假如系统忽略新的 ARP 条目，则局域网上新的结点不能再联络。假如丢掉老的 ARP 条目，结果是网络性能会更慢，因为对每个系统要发送的分组经常需要 ARP 查询。

（2）DoS 攻击

新的 ARP 回答对 ARP 表中老的 ARP 回答进行重写。假如这是用一个坏的 MAC 地址重写，那么将来连接到重写的结点的 IP 地址将失败，因为它将送到错误的 MAC 地址。

（3）MitM 攻击

MitM 攻击通过一个敌意的结点路由所有的通信。和 DoS 攻击类似，ARP 表的条目用不同的机器的 MAC 地址重写。在这种情况下，新的结点将接到所有指向老的结点的通信。通过损坏两者，敌意结点能建立一个成功的 MitM，如图 6-4 所示。

3. 缓解 ARP 的受损

虽然 ARP 受损攻击仅限于本地网，ARP 分组并不通过网桥、路由器或网关。ARP 攻击范围是有限的，但仍然影响网络安全。限制 ARP 攻击影响的方法包括硬编码 ARP 表、ARP 条目超时、过滤 ARP 回答以及锁住 ARP 表。

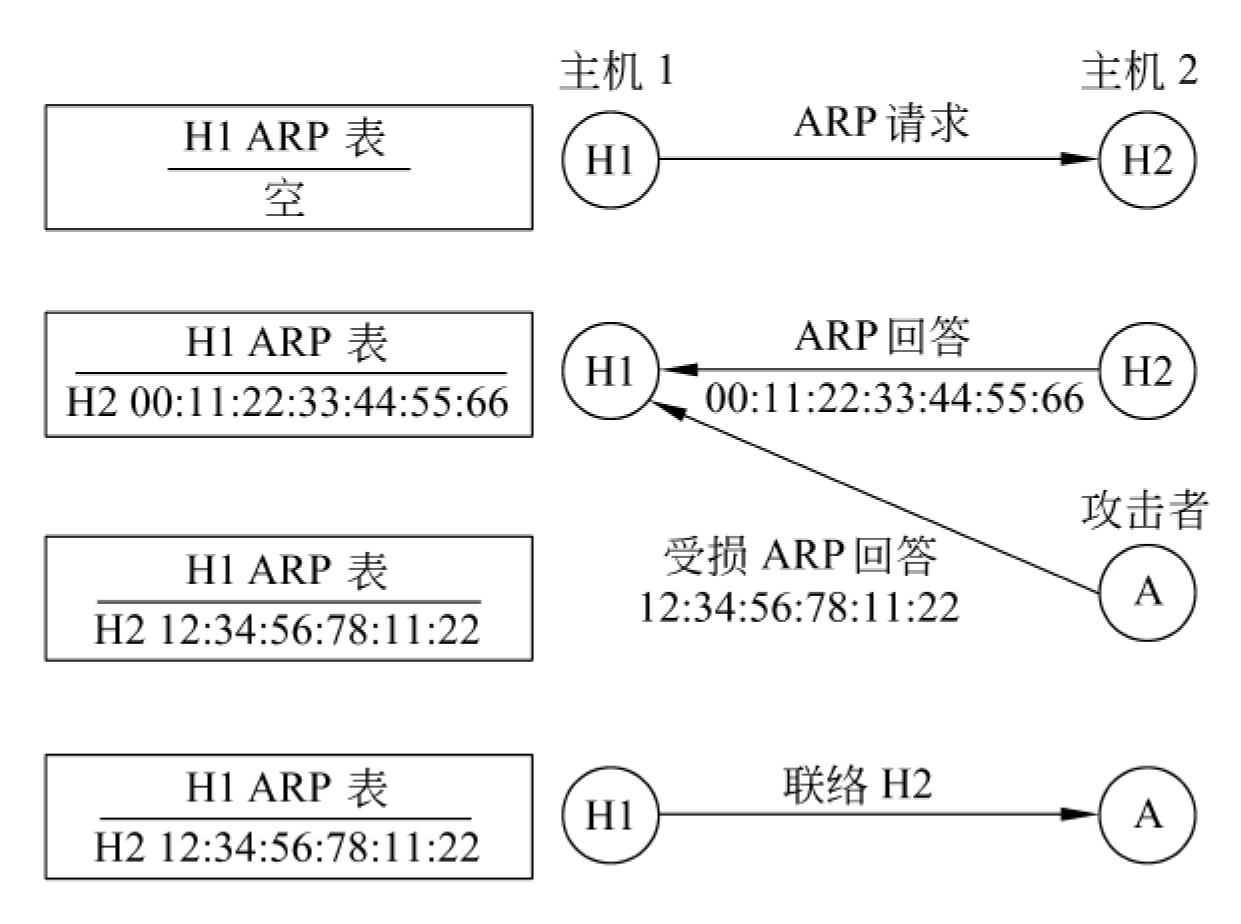


图 6-4　作为 MitM 攻击的 ARP 受损

(1) 硬编码 ARP 表

通常收到每个 ARP 回答时，动态产生 ARP 表，然而利用操作系统命令 arp，可以静态产生 ARP 表。这个命令静态设置 MAC 地址和 IP 地址对到 ARP 表，并阻止进一步修改。

(2) ARP 过期

在 ARP 表中缓存条目可以超时，对超时的条目，MAC 地址和 IP 地址对可从 ARP 表中移走。该方法仅能限制资源攻击的影响。

(3) 过滤 ARP 回答

并非每个 ARP 回答必须插入 ARP 表。Linux 和 BSD 仅对本地主机送来的 ARP 请求缓存条目。这可阻止未经请求的 ARP 回答进入 ARP 表。但 Windows 操作系统接受未经请求的 ARP 回答，并将其插入 ARP 表。虽然 ARP 回答过滤能阻止未经请求的条目，但它并不阻止来自重写已有条目的新的回答。

(4) 锁住 ARP 表

ARP 表能暂时锁住。在这种情况下，一个已经建立的连接能在短期内锁住 ARP 表条目。在这期间，新的 ARP 回答不能重写已经锁住的表条目，以确保已建立的连接不能改变，从而缓解了 MitM 攻击。MitM 攻击只能在极短时间内有可能启动，即系统的 ARP 请求到启动网络连接这一短暂片刻。

4. 交换机攻击

交换机和网桥的网络结点易受中毒攻击和淹没攻击。

(1) 交换机中毒攻击

交换机保持一些 ARP 表以路由通过交换机到特定的物理网络端口的通信。ARP 中毒攻击能破坏 ARP 表。中毒的 ARP 回答能和不同端口的另一个结点的 MAC 地址联系起来。这就有效地将受损结点从网上隔断，本来打算送到受损结点的所有通信会通过攻击者的端口。因为交换机中毒后重新引导网络通信，使攻击者得以拦截连接。

(2) 交换器淹没攻击

在正常情况下，交换机和网桥保证结点只接收到本地物理网的通信。攻击者利用

ARP 中毒能淹没交换机的 ARP 表。因为交换机承受不起这么多的分组，大部分交换机当交换机和 ARP 表满时，退回到 hub 状态。在这种状态，所有结点接收所有通信，运行在随意状态的结点能接收通过交换机的全部网络通信。

大部分网桥和高端交换机支持静态 ARP 条目，使用静态 ARP 表时，这些网络设备就能缓解交换机淹没和中毒的影响。

6.7　网络层风险及安全

6.7.1　路由风险

网络路由器用于和远距离网络通信的一种可选方案。对路由器的直接攻击至少会干扰和其他网络通信的能力。即使物理和数据链路层未受损，网络层能受损，以阻止网络路由。

基于路由器的攻击有以下几种方式：直接攻击、表中毒、表淹没、度量攻击以及路由器环路攻击。

1. 直接路由器攻击

直接路由器攻击有 DoS 和系统破坏两种方式。DoS 阻止路由器执行基本路由任务，使网络不能有效地连接。大部分是基于负载攻击，假如在特定接口的网络值太高，路由器将无法管理通信，包括来自其他网络接口的通信。

路由器损坏虽然很少见，但是可能的。路由器能配置成转发通信到不同的主机，阻断来自特定主机的通信，或任意分配新的子网。因为路由器扩展多个子网，受损的路由器会影响连到它的每个网络的完整性和隐私性。

2. 路由表中毒

少数网络协议对网络通信进行身份鉴别，伪造的或受损的网络通信能重写、插入或移去路由表的条目，其结果是和受损路由器没有多大区别。

网络层协议支持动态路由表，基于观察到的通信自动生成和更新路由表。这类协议更易受攻击，因为其一，新结点可能生成中毒数据；其二，很少动态结点是可以验证的。关键路由器应使用静态路由表以阻止中毒。

3. 路由表淹没

路由器通常没有大的硬驱动或 RAM 来存储路由表，路由表的容量是有限的。如果不用静态路由，设备要管理路由过期和路由表满。攻击者可生成假的数据，路由器用它来生成路由表。当路由表满时，路由器有 3 种选择：忽略新的路由、清除老的路由，或清除最坏的路由。清除新的路由，虽然攻击者无法清除已建立的表条目，但阻止了新的有效的条目插入路由表。清除老的路由，使大的淹没攻击能将已建立的表条目都清除。清除最坏的路由，可使一些理想的路由改成别的路由。大部分动态路由表也支持静态条目，关键路由应配置成静态。

4. 路由度量攻击

路由度量攻击使路由表的动态度量中毒。这种攻击可使一些好的通路似乎成为不期望的。例如，网络层协议支持质量服务 QoS 分组，采用流控决定连接质量。攻击者可伪造 DoS 分组来修改动态度量，结果是更慢的吞吐量、更长的路径和更昂贵的网络开销。

固定路径应使用静态度量。对动态度量是关键的网络，应调整刷新速率，使路由器能经常检查期望的路由。

5. 路由器环路攻击

很多网络协议企图检测和阻止网络环路，因为它会引起过多的频宽消耗，从而消耗掉所有可用的网络频宽。诸如 BGP(Border Gateway Protocol)和 RIP(Routing Information Protocol)都提供检测网络线路的方法。

当网络路由器识别了一个网络环路，就将该路径从路由表中移去。而环路攻击者产生一个假的回答给环路检查，使路由器虚假地认为是网络环路。结果是一个理想的网络路径被去除。虽然静态度量能阻止路由表和度量攻击，但环路攻击仍然能切除预期的路径。

6.7.2 地址机制的风险

网络层并未定义对地址的身份鉴别和验证。基于数字的和名字的地址机制容易受到假地址和拦截的攻击。

1. 假地址

当两个结点有相同的网络层地址，就会产生冲突。但是对高可用性的簇(cluster)，两个结点有相同的网络地址是可行的，当一个结点不能用时，另一结点接收网络通信，使数据不丢失。但假地址能阻止结点接收分组，导致网络连接中断。

2. 地址拦截

当同一子网上两个结点具有相同的网络地址，则响应快的结点能维持网络连接，如果一个结点一直响应慢，则所有网络通信被锁住。具有快的结点的攻击者可以在随意模式下观察网络通信，假如和另一结点具有相同网络地址，则可拦截已建立的网络连接。

当用户不经意地将计算机地址配置成已经使用的网络地址，最坏的情况是将路由器的本地网络地址分配给一个快速工作站，就会有效地阻止网上所有结点和该路由器的通信。

3. 假释放攻击

大部分动态地址分配机制提供地址再分配的方法。当一个结点不需要网络地址时，可通知分配服务器释放该地址，并可分配给其他结点。假释放攻击是攻击者伪装一个已分配的地址，并释放它。结果是受害结点开始运行一个未分配的网络地址，造成假地址攻击。

4. 假的动态分配

当一个结点需要一个新的网络地址时，它必须首先和分配服务器联系。攻击者可以

配置自己的分配服务器，并且响应分配请求比原来的分配服务器更快。

分配响应通常包括一系列的配置信息，例如，DHCP 通常提供一个 IP 地址、掩码地址、默认网关以及 DNS 服务器列表。攻击者能有效地提供假信息给新的结点，并建立一个基于网络路由器的 MitM 攻击。

6.7.3　分段的风险

所有分段机制有两个主要风险：丢失分段和组装数据的容量。此外分段管理的类型能导致丢失数据分段。

1. 丢失分段攻击

一个大的分组要等接收到全部分段才能处理，每个分段必须保存在分配给堆栈的内存中，而内存的容量通常是有限的。当内存满时，就无法接收更多分段分组。

丢失分段攻击发生在当一个大的分组分段时，有一个分段永远未传递。这个攻击会消耗分配给网络协议的资源。为此通常设置一个分段超时值，譬如 30 秒。这意味着分段攻击至少在 30 秒内必须重复，以有效消耗系统资源。这个值对不同操作系统是不一样的。

此外，大部分系统分配一个最大内存大小用于分段组装。假如分段数据的总量大于最大分配内存，那么分段被丢弃，直到超时为止。这将导致处理分段的临时 DoS。

对丢失分段攻击有潜在受攻击的系统，超时和内存分配值能修改，以达到最佳值。

2. 最大的不分段大小

很少分段管理机制传输整个分组，通常结束分段分组用来标识最后的分段。因为整个分组大小是未知的，网络协议应能接收最大的重组分组。例如，IP 报头规定 13 位作为分段偏移(offset)，这就意味着最大的偏移值是 16 383 字节。连同最大的 IP 数据大小为 65 471 字节(65 535 字节分组减去 64 字节报头)，IP 分段机制在分段以前的最大数据大小为 81 854 字节。IP 不能传输大于 80KB 的单个数据块。大部分标准协议规定数据长度小于这最大值。

3. 分段重组

分段须标识以说明分段的次序。有两种情况导致潜在的攻击：分段重复和分段覆盖。如果同样的分段 ID 出现两次，就造成分段重复，也有可能重复的分段包含不同数据。有 3 种选择可实施：忽略第二次分段，在第一次分段上重写，以及作为差错清除所有分段。

诸如 IP，IPv6 协议规定分段偏移，但偏移覆盖会产生和分段重复相类似的情况。

6.7.4　质量服务

因为网络通信中继通过未知的主机，网络结点无法区分真的 QoS 分组和伪造的分组。攻击者可能利用 QoS 功能来隐藏或拦截网络通信。

网络层提供建立和释放网络连接的功能，也保证相同结点间建立多个连接，而不会产生通信干扰。连接管理包括传递确认和面向连接的各种服务。

假的分组可以请求一个结点降低速率或发送更小的分组,导致损坏通信性能。

攻击者可以将已建立的网络,连接重新指向一个不同的远程主机,这可以导致 MitM 或拦截攻击,最坏的情况能引起 DoS 攻击。

假的差错报告能引起过早地使连接断开(DoS)。此外,有些工具能跟踪防火墙内的主机,在已建立的连接复制分组,并改变 TTL。由于 TTL 超时产生的差错返回至呼叫者,这使攻击者能在远程网上进行侦察。

结点的状态能用于简单的侦察,阻止目标可达和导致更多危害的攻击。最简单的分布拒绝服务 DDoS 是 Smurf 攻击,在这个攻击下,一个主机能生成很多回应(echo)请求,送到网上很多主机,每个回应请求指定一个伪造发送者——DDoS 的目标。其结果是回应回答炸弹送至目标结点。足够大的攻击能摧垮大的网络,因为大量的回应回答的产生。

任何能伪造重置分组的攻击者能有效切断网络连接。这些攻击的有效性是基于网络协议。例如 IPv6 使用密码来加密网络连接,这使攻击者很难成功伪造一个重新指向或重新设置分组。IP,IPX 这些协议,相对来说只有较弱的保护。

6.7.5 网络层安全

网络层提供很多服务,以确保成功的互联网数据传递,但它没有描述网络安全传输的方法,大部分网络层协议没有实施身份鉴别、验证及保护网络数据。网络层面临的风险包括窃听、伪装以及插入攻击。

大部分网络层协议对来自低层的风险,诸如数据链路拦截和回答攻击没有提供缓解方法。它假设安全预防措施由高层协议实施。虽然很少有密码解决方案,但是很好地选择网络体系结构以及过滤应用能缓解很多安全风险,此外网络的不兼容能阻止某些安全攻击风险。

1. 安全协议

网络层并不定义安全预防方法,安全由某些专门的网络协议解决。像 IP,IPX 这些通用协议只提供简单的检查和,虽然它能检测某些数据差错,但对检测攻击者没有多大用。

少数网络层协议描述包括安全可选方案。IPv6 和 IPSec 是两个著名的安全协议例子。IPSec 是一个附加在 IP 上的面向安全的协议,包括身份鉴别报头、数据封装以及密钥交换方法。

IPv6 不同于 IPSec,后者是 IP 协议的扩展,前者完全是重新设计的。除了 IP 地址空间的扩展,IPv6 包括加密的身份鉴别和数据封装。

2 网络不兼容能力

大部分网络应用包括管理传输和网络层协议。例如,从 IP 转换到 IPX 会使网络无法实施 Web 浏览,电子邮件和其他面向网络的工具。

虽然 IPv6 支持数据加密,但很多高层协议和应用不支持 IPv6。网络层可以提供各种安全特点,但有些高层协议却不能访问。

3. 体系结构

物理网拓扑结构提供某些内在的安全特点。限制访问物理层可减少窃听、拦截、回答攻击的风险。攻击者如果看不到网络通信，就只能盲目攻击和猜测攻击网络。

虽然数据链路层具有身份鉴别和加密隧道的安全，诸如 CHAP 或 VPN，但它们仅仅保护数据链路连接。敌意的网络层通信能进入数据链路隧道，和正常的网络层通信一样得到允许和保护。

4. 安全过滤

根据 IP 地址的过滤器操作能缓解某些身份鉴别。例如，基于应用的网络服务器(诸如 iptable 或 tchwrapper)能限制基于客户的 IP 地址的访问。又如，inetd. sec 文件和 xinetd 提供的过滤能限制访问 spawned 服务器。虽然这些方法是在模糊安全的水平，但是攻击者必须知道可接受的网络地址来访问服务器。

5. 防火墙和出口过滤

防火墙能在路由器内实施，并基于 IP 地址限制访问。路由器不是路由所有通信，只有来自专门网络接口的通信能访问。虽然远程攻击者伪装不同的 IP 地址，但它们并不能接收和回答，除非它们在目标主机和伪装网络之间的路径。

过滤入口通信能减少伪装攻击的成功，但它并不能阻止来自源点伪装的网络。出口过滤能基于网络地址限制分组中继。例如，假如路由器链接 10.1.X.X 子网到 192.168.X.X 子网，那么它不期望能看到以 192.168 开始的 IP 地址到 10.1.X.X 的接口。出口过滤器对来自正在网络间路由的显然不正确的分组进行阻断。

6.8　IP 风险

虽然 IP 被广泛使用，但它包含一些基本的缺陷，导致不安全风险。这些风险包括地址冲突、拦截、回答攻击、分组风暴及转换通道。实施的疏忽会引起其他风险，诸如分段攻击。

1. 地址冲突

在整个 Internet 上，两个结点不能共享相同的网络地址。假如一个结点被赋值一个 IP 地址，但存在于错误的子网，那么就无法路由。假如在同一子网上的两结点有相同的网络地址，那么路由就有两种可能。

在这种情况下，机器响应较快的，会锁住更慢的系统，因为 IP 只跟踪第一个接收的分组。但是假如采用网络交换机，那么，慢系统会锁住更快的系统，因为如前所述，被较慢的主机发送的分组破坏了交换机的 ARP 表，它将所有通信重指向较慢的结点。

2. IP 拦截

IP 拦截发生在一个结点假装为另一个结点的 IP 地址，通常有 3 种方法实施 IP 拦截，第 1 种是攻击者用未在用的地址拦截，而不会发生冲突；第 2 种是重新指向拦截，攻击者

能重指网络连接到其他主机;第 3 种是随意拦截,沿着网络通路的一个结点能拦截和响应 IP 分组,只要攻击者位于源结点和目的结点之间的通路上。

很多系统根据 IP 地址作为身份鉴别的机制,而拦截 IP 地址的能力限制了这种访问控制系统的有效性。

3. 回答攻击

IP 是一种无状态的协议,这意味着攻击者可以在任何时间记录和回答分组。虽然高层协议可以识别和拒绝 IP 内容,但 IP 数据仍然是有效的。

4. 分组风暴

分组风暴是一种常见的攻击,通信淹没了整个网络。有一类分组风暴称为放大攻击,即一个分组请求能产生一系列的回答,当 ICMP 请求送给一个广播地址,就能产生大量的回答,这就导致基于放大攻击的分组风暴。

另一类分组风暴发生在网络设备不正确处理 ICMP 差错。这在 RFC 1812 中有各种规定以防止这类分组风暴。如用户不按该指南做,就有可能产生很多 ICMP 差错,并淹没网络。如有两个这样的结点存在,就会相互放大差错,最后消耗掉所有可用频宽,将导致摧垮的分组风暴。

5. 分段攻击

IP 支持将大的数据分段传输和在接收端重新组装的能力。这个概念是很简单的,但是很多实施易于出错。两个分段攻击的例子是 Teardrop 和 Nesta。这种易攻击性时常发生在新的网络设备。前者是当诸如 Linux 或 Windows 操作系统重组分组时复制所有的数据到新的内存位置。虽然它们做检查以确保不复制太大的分段,但忽略了分段重叠的情况。后者是利用在很多网络堆栈中的一些漏洞,主要是摧垮 Linux 系统和某些路由器。目前 Teardrop 攻击比 Nesta 攻击更普遍,而且影响大多数操作系统。

6. 转换通道

ICMP 是一个控制协议。很多防火墙和 IDS 系统在中继通信前只是对 ICMP 报头执行一个基本的检查,经常并不详细检查 ICMP 分组的内容。这意味着 ICMP 能不经检查地通过某些防火墙和 IDS 系统。这使 ICMP 成为传送转换信息的理想工具。

6.9　IP 安全可选方案

IP 是最通用的网络层协议,在 Internet 上的任何系统必须支持 IP。虽然 IP 有很多基本的缺陷以及实施时疏忽引起的易攻击。但缓解风险的方法还是有的,包括对不必要的特点禁用,使用非路由的 IP 地址,过滤 IP 通信,以及应用面向安全的协议(可能的情况下)。

6.9.1　禁用 ICMP

虽然 ICMP 提供测试、流控和差错处理,但并不提供网络路由的基本功能。因此,从

安全方面以及更有效角度考虑，可以完全不用 ICMP 支持。

但是大部分操作系统并不提供完全禁用 ICMP 的方法，因此，ICMP 需要在防火墙双向过滤。

6.9.2　非路由地址

无须直接连到 Internet 的主机可用非路由网络地址。RFC 1597 定义了一系列不能路由的子网。这些子网用于私用网。表 6-1 列出了非路由子网。

表 6-1　非路由子网

地址范围	类　别
10.0.0.0—10.255.255.255	A 类
172.16.0.0—172.31.255.255	16 个 B 类
192.168.0.0—192.168.255.255	256 个 C 类

采用非路由网络地址，使攻击者不能直接访问被保护的主机。因为安全不是基于防火墙和过滤，假如防火墙配置错误或不能用，主机是从网上隔离开，而不是直接受攻击。Internet 访问私用网可以通过双主代理或网络地址转换(NAT)提供。

6.9.3　网络地址转换 NAT

NAT 是通过公共网关将来自隔离网的分组中继，NAT 网关是桥接 Internet 和专用网的双主机系统。对每个出口分组，NAT 服务器在内部中继表存储映射关系。中继表包含 3 个成分：源 IP 地址和传输层端口，目的 IP 地址和传输层端口，NAT 服务器外部接口的端口号。使用 NAT 服务器外部 IP 地址和端口号将分组中继到外部网络。外部目的主机视分组来自 NAT 服务器，而非内部系统。

当 NAT 服务器接到来自外部网络接口的分组，它将分组目的地和内部中继表进行比较。然后将分组转发到内部源。

使用 NAT 服务器，很多专用主机通过相同的外部 IP 地址中继。NAT 服务器提供两个安全效果：匿名和隐私。

因为所有通过 NAT 服务器中继的分组好像都来自 NAT 服务器，因此，内部源是匿名的。攻击者无法知道哪个系统是通过 NAT 服务器向外连接的。

攻击者不能连接到内部主机。任何到 NAT 服务器外部接口，但没有内部中继表条目的分组都被丢弃，因为 NAT 服务器不知道如何路由该分组。这使 NAT 成为很有效的防火墙，以阻断无效的外部通信。

6.9.4　反向 NAT

NAT 最大的缺点是不能作为一个主机，因为所有网络通信必须从来自专用网内启动，NAT 服务器不能在专用网内部常驻。因此，NAT 不能用于 Web，E-mail 和其他网络

服务。RNAT 提供从 NAT 服务器的外部端口到专用网上的 IP 地址和内部端口的静态映射。使用 RNAT，外部连接到 NAT 服务器的端口 80(HTTP)能路由到专用网上的 Web 服务器。很多家庭防火墙提供 NAT 和 RNAT 两种服务。NAT 提供防火墙功能，而 RNAT 允许面向服务的应用。

6.9.5 IP 过滤

大部分非 NAT 防火墙支持基于 IP 分组头的分组过滤。过滤器的规则能限制基于特定主机、子网或服务类型(也就是 TCP，UDP 或 ICMP)的分组。这种过滤能应用到源或目的地址以提供在 IP 上的最大控制。

如前所述，ICMP 应禁用，IP 过滤防火墙易于配置成丢弃所有 ICMP 分组，有效地过滤了不希望的通信。

第 3 层的防火墙仅能看到 IP 报头，第 4 层防火墙才能过滤基于特定端口和服务的分组。后者可用于限制访问 Web 或 E-mail 服务器。Web 请求能到达 Web 服务器，只有 E-mail 能到达 E-mail 服务器。

6.9.6 出口过滤

大部分防火墙配置成限制从外面进入的通信，而对出口通信无限制。这种配置一方面提供了最大的安全以防外部的攻击者，另一方面对内部用户提供了最大的方便。但是这种配置允许在内部网络的攻击者对外部资源进行攻击。

出口过滤将防火墙规则应用到出口通信。最简单的出口过滤运行在网络层，以阻止来自内部网络有假的源地址的分组。更加复杂的出口过滤在高层实施，如在传输层限制端口访问，在高层限制 DNS 和 LDAP 访问 VPN 和 SSL 身份鉴别，Web URL 访问、E-mail/SPAM 过滤，病毒扫描等。

6.9.7 IPSec

IP 的主要安全问题是身份鉴别、验证和隐私。IP 没有身份鉴别、没有验证，也没有隐私。

IPSec 是网络层安全标准的集成。使用 IPSec 的两台主机能使用身份鉴别和加密网络协议进行通信。身份鉴别可以基于网络层主机、子网、服务类型、传输层端口或应用层用户实施。不像 IP，高层协议不需提供自己的加密，也无须修改就可用 IPSec，这使 IPSec 成为安全连接和 VPN 的理想解决方案。

6.9.8 IPv6

IPv6 和 IPv4 有很大不同，它包含不同的报头格式，有很多重要的改进，包括扩大的地址空间；支持路由组播和广播分组；在网络层身份鉴别和加密连接的功能，且高层协议可在加密通道上使用而无须修改协议，支持封装以允许网络隧道，加密和身份鉴别一起，提供了完整的 VPN 解决方案。

从安全方面看，IPv6 和 IPSec 本质上是相同的。两者都提供强的身份鉴别、加密和 VPN 支持。很多 IPSec 和 IPv6 的特点都是基于相同的 RFC 规范。

从可行性方面看，从 IPv4 转换到 IPv6，路由器和网络设备必须更新以支持 IPv6 协议。很多新的系统可立即支持 IPv6 或有 IPv6 驱动器可用，但是老的路由器需要更换。相反任何支持 IPv4 的路由器也能支持 IPSec，IPSec 仅需要源和目的站支持，而无须中间系统支持。

6.10　匿名

6.10.1　匿名的属性

网络层允许位于不同子网的两个结点通信。在网络之间传送的数据提供识别发送者和接收者的方法。例如，IP 分组包含一个源和目的 IP 地址。大部分网络协议本质上并不支持匿名网，但通过不同的路由和隐藏技术是可行的。虽然隐私和匿名有相似之处，但它们是不同的概念。网络隐私阻止观察者看到网上传输的信息，而网络匿名是阻止识别连接的参与者。SSH，SSL 和 IPSec 是网络隐私的例子，但它们并不提供匿名。同样，网络匿名系统，诸如代理、盲投并不提供隐私。

网络匿名各有 3 个不同属性，即源匿名、目的匿名和链路匿名。源匿名阻止观察者识别数据传输的源地址，甚至目的主机也不能识别源地址。模糊源地址的能力对双向通信和允许伪装都有影响。无连接的网络服务是用于源匿名的理想方法，因为接收者无须知道源地址。面向连接的网络服务期望双向通信，例如，地址是匿名，发送者就无法得到期望的回答。因此，发送者匿名要通过中继系统实施。伪装不仅允许发送者保持匿名，而且允许攻击者误导任何对它的搜索。跟踪基于假发送地址较跟踪无效地址更困难。

虽然隐藏发送地址仍然允许分组传递，但是隐藏目的地址就更困难了。在网络报头内没有特定的目的地址，分组无法路由和传递。对隐藏目的地址有 3 种方案：广播、拦截和高层中继。

即使发送者和接收者是未知的，但这种访问关系也是可跟踪的。例如，路由器中继网络间通信，通过监控路由器，攻击者能搜索到源和目的子网。虽然不能知道发送者的主机，但能跟踪匿名分组使用的通路。通过短时间的处理和经常改变网络可抵御这种跟踪。

6.10.2　网络匿名

有很多方案可提供网络匿名，最简单的方法是移动地址或盲投(blind drops)。代理和专门的路由网络可提供高层中继。

最简单的发送者匿名是使用移动寻址。发送系统在同一子网上用不同的网络地址临时配置，临时配置用于匿名连接，当连接完成后，源网络地址换到一个没有用过的地址。

只有日志可记录这新的系统，而不出现在子网，有的匿名用户还可考虑改变子网。因为 IP 地址和子网都改变，要跟踪该系统很困难。

盲投是一个源站和目的站都可访问的中间系统。当发送数据时，匿名发送者将报文存储在盲投系统，随后，目的站连接到盲投系统并检查报文。这种系统保证发送者和接收者都匿名。盲投有两个主要的缺点，即速度和识别。除非两者同步，否则速度很慢。观察者能识别盲投，除非用密码能阻止观察者拦截和看到盲投系统的内容。

代理的作用是作为协议中继、转发发送者到接收者的报文。发送者能连接到代理，仅利用代理的网络地址到目的站。代理使发送者匿名。在代理和目的站之间的观察者能看到连接，但不能识别发送者。相反，位于发送者和代理之间的观察者通常不知道连接的目的站。除了提供匿名外，代理通常可用于一个组织网络的出口过滤。代理足够快，可提供实时连接。但是很多代理服务器有连接日志，可识别发送者、接收者和未加密的内容。在内部的观察者，还是能识别目的站及传输内容。

代理只提供一级迂回来分割源和地址，虽然代理服务器能构成链，但链是静态的，且大大影响速度，每个分组必须通过代理服务器中继，而不是沿着最优的路径。更严重的是在任何代理上的攻击者通过观察数据内容或连接序列能识别源和目的。路由网络（诸如网格（mesh）、格栅（grid））和洋葱头（onion）路由是不同于代理的另一种方案。前两种路由网络包含事先确定的型式安排的中继。格栅网络将每个结点放置成格栅型式。虽然典型的格栅网描述成每个结点包含 4 条链路到其他结点，但格栅网可以是 3 个自由度（或 n 个自由度），结点可安排成各种几何型式。网格网络可包含不同数的链路，但每个结点至少连接到两个其他结点。这两种网络的基本概念是冗余的，从匿名观点看，它们运行在网络层，可模糊发送者、接收者和连接内容，在任何一个中继的攻击者看不到通信，或仅能看到部分通信。但这两种网络，都是网络决定路由，假如一个结点不可用，则数据经过别的路径路由。而洋葱头路由由发送者选择路径，采用数据编码和公钥，第 2 代洋葱头路由器 Tor 就是这种实例，可提供源、目的和链路匿名。

6.10.3　网络匿名的局限性

大部分匿名系统是基于网络层保护身份的识别，然而一些网络层以外的因素也能导致身份识别：

- 高层信息泄露：高层含有的身份识别信息会危害匿名连接。
- 时序攻击：攻击者知道时序后可优化其攻击以跟踪匿名连接。
- 习惯和序列型式：和时序攻击类似，习惯形态和序列访问能识别匿名用户。

此外匿名还有一些漏洞，例如，使用 cookies 可允许攻击者在线跟踪用户；给匿名目标发送一个 web bug，攻击者可造成匿名漏洞；攻击者发送一个唯一的主机名给匿名目标，然后观察 DNS，能识别目标网络地址；匿名下载有可能传送敌意码到匿名发送者和接收者，进而造成特洛伊木马攻击和回叫炸弹。

6.11 本章小结

不同类型的漏洞、攻击和威胁存在于 Internet 的不同层次，Internet 安全体系结构就是对不同类型的攻击实施不同层的保护，本章重点分析物理层、数据链路层和网络层的风险以及缓解风险的方法。

对 LAN 的物理网攻击包括连接破坏、干扰和故意攻击。防御的方法用防火墙将网段分隔开来，定义不同的特权区以及采用安全的动态 LAN 链接。

无线网的风险包括分组嗅测、SSID 信息、假冒、寄生和直接安全漏洞。缓解风险的方法有 SSID 打标签、广播 SSID、天线放置、MAC 过滤、WEP 协议以及安全的网络体系结构。

数据链路层的风险包括随意模式的监控、负载攻击、地址攻击、帧外数据以及转换通道。缓解风险的方法有硬编码硬件地址、数据链路层和高层的身份鉴别机制。

PPP 的主要风险是身份鉴别和双向通信。MAC 的风险是硬件框架攻击、伪装攻击和负载攻击。ARP 的主要风险是 ARP 表的受损。

网络层的风险包括路由风险、地址机制风险、分段风险和质量服务(QoS)攻击。缓解风险的方法有采用安全协议、网络不兼容能力、网络体系结构、安全过滤以及采用防火墙和出口过滤。

IP 风险包括地址冲突、IP 拦截、回答攻击、分组风暴、分段攻击以及转换通道。IP 安全可选方案有禁用 ICMP、采用非路由地址、网络地址转换 NAT、反向 NAT、IP 过滤、出口过滤、IPSec 以及 IPv6。

习　　题

1. 列出物理网风险的 4 种类型。
2. 什么是身份鉴别栈?
3. 列出对有线物理网攻击的 5 种类型。
4. 有哪几种动态 LAN 链接的身份鉴别方法?
5. 列出无线网的各种风险。
6. WEP 是一种高强度安全方法吗? 为什么?
7. 什么是数据链路的随意模式?
8. 列出各种缓解数据链路层风险的方法。
9. 试述 CHAP 的功能、特点和局限性。
10. ARP 为什么会受损? ARP 受损后有何影响? 如何能缓解 ARP 受损?
11. 基于路由器的攻击有哪几种? 路由表淹没后有哪几种结果?
12. OSI 网络层是否定义地址的身份鉴别和验证? 基于数字和名字的地址机制容易受到何种地址攻击?

13. 什么是分段机制的主要危险？假如分段组装超时值设置过低会有什么后果？

14. 网络层提供哪些 QoS 功能？QoS 攻击有哪些？

15. 网络层有哪些安全风险？网络层安全风险缓解方法有哪些？它们有哪些局限性？

16. 什么是 IP 的安全风险？

17. 比较各种 IP 安全可选方案的优缺点。IPSec 和的 IPv6 的异同是什么？

18. 网络匿名的方案有哪些？有何局限性？

第7章 Internet安全体系结构之二

本章要点:

- 传输层风险及缓解方法;
- 攻击TCP和UDP的方法及缓解方法;
- DNS风险及缓解方法;
- SMTP邮件风险及缓解方法;
- HTTP风险及缓解方法。

不同类型的漏洞、攻击和威胁存在于Internet的不同层次,Internet安全体系结构就是依照层次结构的原则,对不同类型的攻击实施不同层的保护。本章重点分析传输层和应用层的风险以及缓解风险的方法。

7.1 传输层核心功能

传输层定义网络层和面向应用层之间的接口,从应用层抽象连网功能,包括连接管理、分组组装和服务识别。为实现这些功能,传输层有两个核心成分,即传输层端口和序列。

7.1.1 端口和套接字

传输层使用网络层来建立结点之间的连接,网络层路由提供网络套接字。套接字有主动的和被动的两种。主动套接字指示建立网络连接,服务器使用被动套接字,等待和监听网络连接。传输层生成端口,每个端口包含一个唯一的、针对特定高层服务的标识。一个套接字可管理很多端口,但每个端口都需要一个套接字。端口和特定的高层协议相关联,或动态分配。例如,Web(HTTP)使用TCP协议的端口80的服务。

大部分远程网络攻击针对特定端口的特定服务为目标。但很多DoS攻击却针对很多端口或套接字为目标。因此,传输层攻击可包括端口、套接字和专门的协议实施。

7.1.2 排序

传输层从高层接收数据块,并将其分成分组,每个分组赋予一个唯一的序列标识,用来跟踪分组。传输层保持一些已经用于端口的序列号表,以防止序列号重复。

因为序列号用于保持传输层的分组传输有序,这构成普遍的攻击因素,排序能用于传

输层拦截攻击。

7.1.3 序列拦截

攻击者要观察传输层分组必须识别序列，以插入或拦截连接。假如伪造者具有有效的序列号，就好似经身份鉴别并被目标系统接受。因此，序列号的产生最好不要依次渐增，否则攻击者易于预测下一个分组的序列号。

随机初始序列号通常用于传输连接的开始，以阻止攻击者猜测第一个分组。但对已建立的传输连接，通常使用分组头指示当前的和下一个序列号。攻击者观察这类分组头，就知道下一个序列号可模仿。攻击者可赋予下一个伪造分组的序列号，有效地锁住已建立的连接。假如传输连接提供已建立的登录，则攻击者可立即得到访问这个登录。

序列号通常起始于随机值，但整个会话过程中逐一增加。观察者很容易识别序列型式并拦截会话，但是盲目攻击者不能识别初始序列号。这样盲目攻击者无法决定序列号以及危害传输层连接。

但是很多传输层协议的实施使用伪随机数发生器，就成为可预测的。随机数发生器的复杂性决定分组序列的预测性，攻击者能建立很多传输连接，并决定初始序列号的型式。这个弱点允许盲目攻击者能危害传输层连接。

有一些解决传输层拦截的方法。大部分需要的安全服务是依靠高层协议来做连接的身份鉴别。例如，SSH 连接能通过 TCP 拦截，但拦截者不能进行身份鉴别或正确地响应 SSH 分组。这种类型的拦截，好像是建立了 SSH 连接，突然又断链。结果是好像阻止了攻击，但无法阻止进一步的 DoS 攻击。

传输层的核心功能还包括连接管理、分组序列以及保持存活等。

7.2 传输层风险

传输层的主要风险围绕着序列号和端口。要拦截传输层连接，攻击者必须破坏分组排序。传输层端口直接导致网络服务。目标瞄准端口，远程攻击者可针对一个专门的高层服务。传输层还能导致侦察攻击，包括端口扫描和信息泄露。

7.2.1 传输层拦截

拦截攻击能发生在任何一个网络层次，而传输层攻击需要两个条件，一个是攻击者必须对某种类型的网络层破坏，一个是攻击者必须识别传输序列。

从攻击者的观点，分组序列号可导致传输层拦截，并有助于重构观察到的数据传输。没有拦截和继续传输序列的能力，分组无法得到回答响应，新的分组也不能接受。例如，TCP 包含分组序列号，下一个序列号以及对上一个序列号的回答响应，并组合在一个分组头内。攻击者观察 TCP 分组头能识别序列的下一个分组以及任何需要回答响应的分组。一般来说，拦截传输层连接的能力取决于序列号的质量。

为了完成一次拦截，攻击者必须伪装网络层通信。伪装的分组必须包含源地址、目的

地址、源端口和目的端口。

如前所述，随机序列号能减少传输层拦截的风险，像 UDP 这种不用序列号的协议，则更易受攻击。

7.22 一个端口和多个端口的比较

减少结点的端口数，能减少攻击因素。加固的服务器将开放的端口数减少到只有基本服务。公共的 Web 服务器仅有 HTTP(80/tcp)打开，远程控制台只有 SSH(22/tcp)打开。

一般来说，少量端口打开的系统更安全。但是某些服务支持多路端口，或基于服务的需求打开新的端口。例如，代理只有一个端口打开，(1080/tcp 用于 SOCKS)，但一个端口可连接很多其他系统以及很多其他端口。又如 SSH 支持端口转发，虽然 SSH 仅使用一个端口，但远程客户可从很多端口将通信转发到 SSH 安全隧道。即使 SSH 隧道是安全的，但隧道的端点可能是不安全的。

7.23 静态端口赋值和动态端口赋值

远程客户连接到服务器需要两个条件，其一，需要服务器的网络地址；其二，需要知道传输协议及端口。

客户启动服务器连接时，通常连接到服务器的众所周知的端口。但有时客户使用短暂的端口，它选自动态端口的范围内。为了使服务器回答客户，客户的分组包括网络地址和端口号。

防火墙使用端口信息提供网络访问。例如，在 E-mail 服务器前面的防火墙允许外部请求路由到特定的内部主机的 25/tcp。而具有出口过滤的防火墙以及 NAT 支持的路由器动态跟踪分组会话。在一个端口上的远程主机能和在另一端口上的本地主机对话。

某些高层协议不使用固定端口号，例如 RPC，FTP 的数据连接以及 Net meeting。不用单个端口于全部通信，控制服务使用众所周知端口，数据传输则用动态端口，启动连接到控制服务产生一个报文以标识动态端口号。

动态端口会引起不安全的风险，因为大范围的端口必须都可访问网络。例如 FTP 生成第 2 个端口以传输数据，动态端口可选用任何未使用的端口号，如果防火墙不打开所有端口，FTP 数据连接就会被阻断。有一些 FTP 通过防火墙的可行方案，但都有隐患或局限。

7.24 端口扫描

为了攻击一个服务，必须识别服务端口。端口扫描的任务是企图连接到主机的每一个端口。假如端口有回答，则活动服务正在监听端口。假如服务是在众所周知的端口，则增加了服务识别的可能性。扫描方法一般有两种，一种是目标端口扫描，用以测试特定的端口，一种是端口扫除(sweep)，用以测试主机上所有可能的端口。有很多种方法可防御端口扫描，包括非标准端口，无回答防御，总是回答防御、敲打协议(knock-knock protocol)、主动扫描检测以及故意延迟等。

很多服务运行在众所周知的端口,易于被攻击者识别服务的类型。如将众所周知的端口移到非标准端口以模糊服务类型,就可防止攻击。但要注意那些端口是未分配给其他服务。

因为端口扫描等待分组回答,某些系统变化回答。例如 BSD 系统对不活动端口的分组请求不予回答。这样使扫描系统等待回答直至超时。

BSD 系统不回答不活动端口,但对活动端口易被攻击识别。改变的方案是总是回答,攻击者就无法区别是活动端口还是不活动端口。

敲打服务器不保持端口打开,而是监控其他端口或网络协议,当观察到期望的分组序列,服务才启动。例如 SSH 服务器先不和端口绑定,直到主机看到具有 700 字节不规划数据字长的 ICMP 分组才和端口绑定。攻击者扫描 SSH 服务不产生需要的 ICMP 分组,也就看不到运行在服务器的 SSH。

虽然采用技术上模糊安全的方法,能有效地延缓攻击者,但主动的安全方案是可行的,IDS 能观察扫描主机的一系列连接并阻断访问。此外还有一些故意设法延迟攻击或延迟建立攻击连接的方法,也能阻止攻击。

7.2.5 信息泄露

一般传输层对传输的数据不进行加密,因此传输层协议本身并不对信息保护。在网上监控分组通信的观察者能观察到传输层协议的内容,通常是在传输层上面的高层提供身份鉴别和加密。

7.3 TCP 侦察

绑定到 TCP 端口的网络服务提供对主机系统的直接访问。假如服务提供对硬驱动的访问,那么任何远程用户就有可能访问硬驱动。通过识别系统的类型和服务的类型,攻击者能选择相应的攻击指向。

7.3.1 操作系统框架

大部分 TCP 的实施允许参数定制以优化连接。系统可以规定更大的窗口大小,定义更多的重试,或者包括像时间戳这些专门的 TCP 选项。这些值的默认选择是由操作系统定的。它能识别专门的操作系统版本和补丁的级别。

1. 初始窗口大小

不同操作系统使用不同初始窗口大小。虽然初始窗口值可修改,但大部分系统还是使用默认值。利用这些信息可识别传输数据的操作系统的类型。当 TCP 会话继续时,窗口大小会增加,而总的增加值多少也是由操作系统确定的。利用这信息,同样也能估算出介入的操作系统类型。

2. TCP 选项

每个 TCP 分组包含 TCP 报头值的一些选项,不同的操作系统支持不同的选项、值和

次序。通过观察这些选项,可识别特定的操作系统。某种情况下,TCP 选项能唯一足够识别操作系统和补丁级别。知道系统补丁的级别对攻击者有很大帮助,因为可识别未打系统补丁的漏洞。

3. 序列号

虽然所有实施 TCP 系统用同样的方法增加序列号,但是初始序列号是各个操作系统特定的。初始 SYN 和 SYN-ACK 分组交换用于连接的起始序列号。虽然单个 TCP 连接不能泄露可识别信息,但是一系列的快速连接能泄露用来建立初始连接的型式。序列号能用来识别操作系统、版本,以及补丁版本的信息。

4. 客户端口号

虽然服务器绑定到固定的 TCP 端口号,但客户可选择任何可用的端口号用于连接。服务器可从 TCP 报头决定客户动态端口号。从客户到一个或多个服务器重复的连接将显示对每个连接的不同端口号。不同的操作系统使用不同的动态端口号范围,供客户选择。观察动态端口号的范围,可以帮助识别操作系统。

5. 重试

当 TCP 分组没有收到回答响应,分组重新发送。重试的次数以及间隔是不同操作系统特定的。可以通过 SYN 重试、SYN-ACK 重试以及 ACK 重试 3 种不同方法来确定。

有一些用于框架系统的通用工具。例如 Snacktime 工具是基于 TCP 窗口大小、选项,以及重试间隔来推算系统的。又如 Pof 和 Nmap 工具,通过询问两个端口来检测服务器 TCP 配置的细微变化。

操作系统框架对诊断技术是有用的,但对攻击者在攻击以前的侦察也是有用的。攻击者使用网络框架来识别执行的操作系统以及补丁级别。改变一些诸如窗口大小、重试超时等默认值,可以阻止攻击者对系统的识别。因为改变系统的默认 TCP 设置不是普遍的,使攻击者从侦察得来的错误信息信以为真。

7.3.2 端口扫描

TCP 端口扫描用来识别运行的服务。端口扫描企图连接到端口并记录结果。对任何连接的企图,一般有 4 种回答的类型:

- SYN-ACK:假如一个服务在端口运行,那么 SYN-ACK 返回给客户,这是正的识别。为了阻止检测,一些防火墙总是返回一个 SYN-ACK,即使没有服务也是可行的。这个对策的结果是使扫描器不能识别打开的端口。
- RST:假如没有服务在运行,很多系统返回一个 RST 分组。这提供一个快速确认:在端口上没有服务。
- ICMP 不可达:假如主机是不可达,那么 ICMP 分组返回以指示失败。这使端口状态未知,因为测试不可达。有些防火墙采用这种方法以迷惑扫描器。
- 什么也没有:假如分组没有到主机,根本就没有回答,SYN 请求得不到 SYN-ACK 并超时,虽然这通常意味着主机不可达或不在线,但一些防火墙有意忽略发送的分组并关掉端口。

7.3.3 日志

为了检测系统扫描和网络攻击，日志是重要的。很多网络服务有连接日志，包括时间戳、客户网络地址以及相关的连接信息。少数系统支持未加工的 TCP 通信，由高层执行日志。在握手完成以前，高层并不支持 TCP 连接，结果使部分端口扫描（在握手未完成以前）常常是没有日志的。

网络监控工具，诸如 IDS 和 IPS，一般监控和日志 SYN 请求以及任何不包括部分建立连接的通信。SYN 分组被记录，未请求的 ACK 和 RST 分组也被日志。基于这些分组的频度、类型和次序，一些工具能识别网络扫描。如果是 IPS，在扫描完成以前就能做出反应，以阻止更多信息泄露以及限制服务检测。假如任何攻击者不能识别系统的类型，那么破坏系统的能力大大减弱。

7.4 TCP 拦截

任何干扰 TCP 连接的攻击都归结为 TCP 拦截，这些攻击常常像 DoS 一样出现，使连接过早地结束。全会话拦截虽然很少，发生在当一个攻击者不仅结束一个 TCP 连接，而是继续把其他连接断掉。TCP 客户接到一个连接结束或 TCP 超时，同时服务器没有注意到攻击者已经替换了没有登记注册的客户。

1. 全会话拦截

全会话拦截常常需要攻击者具有直接的数据链路访问。运行在随意模式，攻击者观察网络地址、端口以及用于连接的序列号。利用这些信息，攻击者试图比一个 TCP 连接结束更快的响应。有时只差微秒时间就能决定是成功还是失败。成功的拦截提供具有连接会话的攻击者到网络服务，而失败的拦截结果造成 DoS 或只是简单的忽略。

2. ICMP 和 TCP 拦截

ICMP 用来在 IP 和 TCP 之间通信。ICMP 能用来报告不成功的连接或重新指向网络服务。遇到恶意使用时，ICMP 能将 TCP 连接重新指向不同的端口和不同的主机。虽然攻击者仍必须知道 TCP 的序列号，但是 ICMP 不需要使用 DoS 来结束任何一个原始连接。

7.5 TCP DoS

DoS 攻击有两个目的，其一是能使受害者不能执行任务，其二是更秘密的攻击，因为 DoS 攻击是十分引人注意的，会很快被管理注意，为此攻击者在对一个系统执行 DoS 的同时，狡猾地又对另一个不同系统攻击，使管理者在集中第 1 个 DoS 时，没有注意第 2 个攻击。

TCP 是十分易于受 DoS 攻击的。任何对端口号或序列的干扰结果都会使连接断开。

虽然拦截能造成 DoS，但它不是唯一的攻击类型。TCP DoS 攻击可来自 SYN，RST 或 ICMP 分组，攻击者无须直接网络访问(随意模式)来执行攻击。

1. SYN 攻击

每个 TCP 实施分配用于管理连接的内存。每个连接包括网络地址、端口、窗口大小信息、序列号以及用于入出分组的缓存空间。当每个服务器收到 SYN 就分配内存。SYN 攻击发送大量的 SYN 分组来消耗可用的内存。假如 TCP 实施只能管理 250 个并发连接，那么超过这个数的连接被切断。

每次 SYN 分组放到一个打开的服务，就产生一个 SYN-ACK 响应，假如握手还未完成，那么连接超时。结果就造成有效的 DoS，攻击者发送大量的 SYN 请求，服务器被切断，直至连接超时。

有一些缓解 SYN 攻击风险的方法，包括增加 SYN 队列，以增加允许的连接数，减少 SYN 超时，以降低 SYN 攻击的影响以及当攻击停止时，可快速恢复；用 SYN Cookies 以防止因 SYN 攻击而消耗内存。

2. RST 和 FIN 攻击

RST 攻击是发送 RST(或 FIN)分组，反常地结束已建立的连接。假如攻击者能看到网络通信，那么，就能插入一个 RST 分组，并断开被害者已建立的连接。

盲目的 TCP 重置攻击发生在当攻击者不能拦截或看到网络连接。伪造的 RST 分组用各种不同的序列和端口值发送。只要其中一个是有效的，就能断开连接。

序列号包含 4 个字节，因此有 4 294 967 296 可能的序列号。事实上，攻击者无须发送 40 亿个分组，因为回答响应窗口有限，就降低了需要的分组数。例如 Windows XP 使用初始窗口大小为 64 240 字节，则只需要发送 66 858 个分组。在 IP 和以太网上的 TCP 产生最小分组大小为 72 字节，假如 10Mbps 的速率，发送 66 858 分组大约只需 5 秒钟。

3. ICMP 攻击

类似于 TCP 重置攻击，ICMP 可用来指定一个断开连接。盲目 ICMP 攻击也能使 TCP 不能连接。不像 TCP 重置攻击，防火墙能阻断 ICMP 攻击，而 TCP 重置攻击则因为有效的端口和地址组合，能通过防火墙。

4. LAND 攻击

LAND 攻击形成反馈环路影响大部分 LAN 守护进程，这种攻击是发送一个 SYN 分组到已知端口的开放服务，而回答地址和端口伪装成指回同一个系统，形成一个反馈环路，使系统很快摧垮。如今的操作系统对 LAND 攻击已能抵制。

7.6　缓解对 TCP 攻击的方法

虽然 TCP 差不多是全世界通用的，但很少厂家使用相同的实施，甚至不同的版本和补丁能导致实施的差异。异构网看来不会被单一的攻击影响，网上每个服务器都有各自

的对付办法。主要实施风险来自单一的实施以及和低层协议的相互作用。缓解的方法围绕着替换系统框架以及检测攻击。

1. 改变系统框架

TCP 和网络服务攻击有两类，即盲目攻击和定向攻击。前者没有假定的攻击目标，通过试探发现漏洞，大部分计算机病毒使用这种方法。

定向攻击针对特定操作系统平台和网络服务。首先通过侦察识别可能的目标，然后攻击可行的目标。通过改变系统框架就可缓解攻击者的识别。不同的框架包括 SYN 超时、重试计数、重试间隔、初始窗口大小、可用的 TCP 选项以及初始序列值。

很多 TCP 端口是标准化的，特定端口用于特定服务。例如端口 22/tcp 用于 SSH，端口 80/tcp 用于 HTTP。虽然这些端口号是标准的，但不是必需的。可以改变端口号以减少攻击的可能性。

2. 阻断攻击指向

防火墙用来限制网络访问，假如家庭网或小的办公室网不提供任何对外网络服务，那么防火墙可阻断任何外部的 SYN 分组。假如 DMZ 仅支持 Web 服务器，那么只有 Web 端口允许通过防火墙。

此外阻断 ICMP 通信能消除来自远程 ICMP 淹没、拦截和重置攻击的风险。

3. 识别网络设备

识别网络设备和已知已受攻击的漏洞，可设法预先防止。对一些简单的设备和家庭防火墙、PDAs 以及具有网络支持的可移动设备，无须所有 TCP 实施以减少攻击风险。

4. 状态分组检验

很多防火墙支持状态分组检验(SPI)。SPI 跟踪 TCP 连接状态以及拒绝和已知状态不匹配的分组。例如，一个 RST 送到关闭的端口，可把它丢掉，而不是传递给主机。SPI 能减少拦截攻击、重置攻击、远程系统框架等的影响。

5. 入侵检测系统(IDS)

IDS 对非标准的或非期望的分组的网络进行监控。IDS 能很快地识别远程系统框架、TCP 端口扫描、拦截企图以及 DoS 攻击。

虽然 IDS 能检测攻击，但这些系统也发送大量虚假的结果，以致淹没管理者。此外如果管理者只是依赖 IDS 报告可能会遗漏网络攻击，有时攻击者会故意使管理者转移视线，以致漏掉真正的攻击。

6. 入侵防御系统(IPS)

IPS 扩展了 IDS 功能，从仅仅是日志记录到采取行动。IPS 能使攻击指向不成功，而采取正确的行动。假如 IDS 识别一个端口扫描，它会立刻阻断其余的扫描以限制扫描的有效性。

7. 高层协议

TCP 不提供对来自低层协议的信息。ARP 以及基于网络攻击能大大影响 TCP。虽然序列号和短暂的端口选择能减少回答攻击的影响，但在插入以前，TCP 报头能被修改。一般来说，假定高层协议将鉴别通信以及检测可能的攻击。

7.7 UDP

UDP 是一个简单的传输层协议，用于无连接服务。因为很多 TCP 功能并非是必需的，UDP 分组有一个简单的报头，仅包括源端口、目的端口、数据长度和检查和，总共 8 个字节。此外 UDP 传输不产生回答的响应。

虽然比起 TCP 来，UDP 只需很少的网络带宽，但它更易受攻击，UDP 攻击常常基于无效的分组以及伪装。

1. 非法的进入源

UDP 服务器不执行初始握手，任何主机能连接到 UDP 服务器，而且连接是无须进行身份鉴别的。

任何类型的 UDP 分组都能淹没一个服务器。服务器缓冲有限数的 UDP 分组。假如接收到更多分组，那么它将被丢弃直到空出缓冲器空间。UDP 分组能很快淹没慢的 UDP 服务。

2. UDP 拦截

UDP 服务器可从任何主机接收分组，而无须进行身份鉴别。这样任何客户能发送任何分组到任何 UDP 服务器。管理任何会话或连接必须由高层协议处理。这意味着 UDP 是十分易于拦截的，攻击者能很容易伪装成正确的网络地址和 UDP 端口，将数据插入到接收者。盲目的 UDP 攻击只需猜测端口号，不超过 65 536，只需几秒钟。

3. UDP 保持存活攻击

UDP 没有很清楚地指示连接是打开还是关闭，结果大多数防火墙当看到第一个出口连接时，打开端口，在不活动一段时间后才关闭端口。攻击者能利用这个弱点来保持 UDP 端口打开。即使客户不在监听分组时，攻击者能发送 UDP 分组到防火墙，以保持防火墙端口打开。假如有足够多的端口保持打开，那么没有新的端口能打开。这使 UDP 不能有效地通过防火墙。

4. UDP Smurf 攻击

前面讲到 ICMP Smurf 攻击，UDP 也易受到这种攻击，假的分组送到 UDP 服务器。攻击者伪造被害者的网络地址作为分组发送者，服务器响应发送一个或更多 UDP 分组给被害者。虽然少数 UDP 分组不会严重影响分组，但每秒几千个分组能摧垮一个网络。

5. UDP 侦察

UDP 对系统框架和侦察只提供少量选项。UDP 端口扫描依靠 ICMP 和分组回答。

假如没有 UDP 服务存在于扫描端口，那么 ICMP 的“目的不可达”分组被返回。但有些 UDP 服务对没有连接返回一个回答。任何 UDP 回答指示一个存在的服务。无回答指示一个服务接收到分组而没有回答。要击败这类端口扫描的唯一方法是不返回任何 ICMP 分组。这使无回答难以区分有没有服务。

7.8　安全套接字层 SSL

由于 TCP/IP 协议本身非常简单，没有加密、身份鉴别等安全特性，因此要向上层应用提供安全通信的机制就必须在 TCP 之上建立一个安全通信层次。传输层网关在两个通信结点之间代为传递 TCP 连接并进行控制，这个层次一般称为传输层安全。最常见的传输层安全技术有 SSL，SOCKS 和安全 RPC 等。

在 Internet 应用编程中，通常使用广义的进程间通信（IPC）机制来与不同层次的安全协议打交道。比较流行的两个 IPC 编程界面 BSD Sockets 和传输层界面（TLI），在 UNIX 系统Ⅴ里可以找到。

在 Internet 中提供安全服务的首先一个想法便是在它的 IPC 界面加入安全支持，如 BSD Sockets 接口等，具体做法包括双向实体的鉴别，数据加密密钥的交换等。Netscape 通信公司遵循了这个思路，制定了建立在可靠的传输服务（如 TCP/IP 所提供）基础上的安全套接层协议（SSL）。SSL 版本 3（SSLv3）于 1995 年 12 月制定。SSL 分为两层，上面是 SSL 协商层，双方通过协商约定有关加密的算法、进行身份鉴别等；下面是 SSL 记录层，它把上层的数据经分段、压缩后加密，由传输层传送出去。SSL 采用公钥方式进行身份鉴别，但是大量数据传输仍使用对称密钥方式。通过双方协商，SSL 可以支持多种身份鉴别、加密和检验算法。两个层次对应以下两个协议：

（1）SSL 记录层协议。它涉及应用程序提供的分段、压缩、数据鉴别和加密。SSLv3 提供对数据鉴别用的 MD5 和 SHA 以及数据加密用的 R4 和 DES 等的支持，对数据进行鉴别和加密的密钥可以通过 SSL 的握手协议来协商。

（2）SSL 协商协议。用来交换版本号、加密算法、（相互）身份鉴别并交换密钥。SSLv3 提供对 Deffie-Hellman 密钥交换算法、基于 RSA 的密钥交换机制和另一种实现在 Frotezza chip 上的密钥交换机制的支持。

高层协议
SSL 协商层
SSL 记录层
传输层
低层协议

图 7-1　SSL 结构图

SSL 的结构如图 7-1 所示。

使用 SSL 协议通信的双方通过协商层来约定协议版本，加密算法，进行身份验证，生成共享密钥等。SSL 协商层的工作过程如图 7-2 所示。当客户方与服务方进行通信之前，客户方发出问候；服务方收到问候后，发回一个问候。问候交换完毕后，就确定了双方采用的 SSL 协议的版本号、会话标志、加密算法集和压缩算法。服务方在问候之后，还可以发出一个 X.509 格式的证书（certificate），向客户方验证身份。随后服务方发出问候结束，表明问候阶段的结束，等待客户方回答。客户方此时也可以发回自己的 X.509 格式的证书，向服务方认证自己的身

份。然后客户方随即产生一个对称密钥,用服务方公钥进行加密,客户方据此生成密钥交换信息传送给服务方。如果采用了双向的身份认证,客户方还需要对密钥交换信息进行签名,并发送证书检验(certificate verify)报文。服务方获得密钥交换信息和证书检验信息后就可以获得客户方生成的密钥。至此,有关加密的约定和密钥都已建立,双方可以使用刚刚协商的加密约定交换应用数据了。

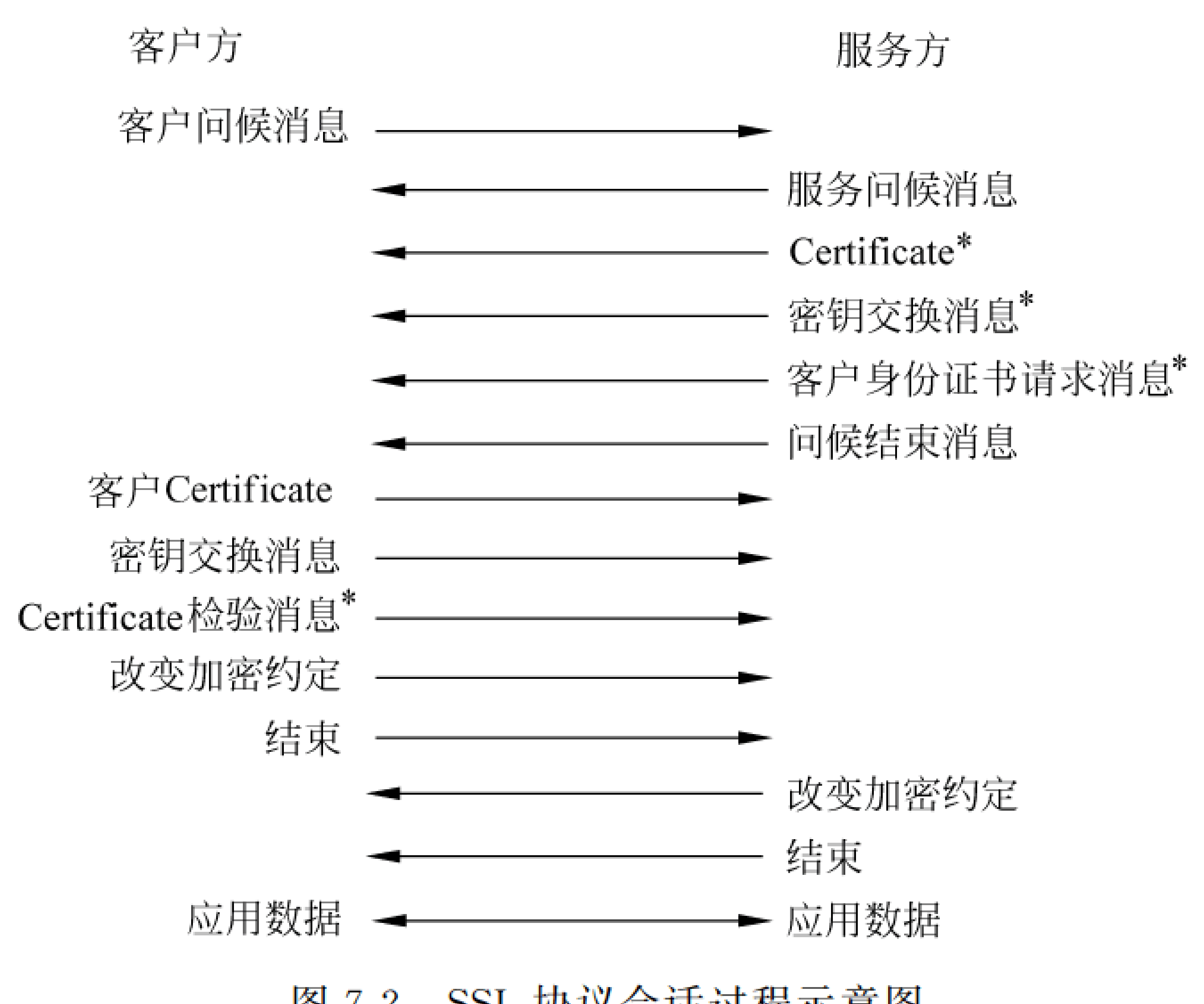


图 7-2　SSL 协议会话过程示意图

SSL 记录层接收上层的数据,将它们分段;然后用协商层约定的压缩方法进行压缩,压缩后的记录用约定的流加密或块加密方式进行加密,再由传输层发送出去。

IP 层安全机制的主要优点是它的透明性,即安全服务的提供不要求应用做任何改变。这对传输层来说是做不到的。原则上,任何 TCP/IP 应用,只要应用传输层安全协议,比如说 SSL 或 PCT,就必定要进行若干修改以增加相应的功能,并使用(稍微)不同的 IPC 界面。传输层安全机制的主要缺点就是对应用层不透明,应用程序必须修改以使用 SSL 应用接口,而且要对传输层建立起安全机制。同时 SSL 也同样存在公钥体系的不方便性,例如用户很难记住自己的公钥和私钥,必须依靠某些物理设备(如 IC 卡或者磁盘)来存储,这样对用户终端有一定要求。再有就是服务方和客户方必须依赖 CA 来签发证书,双方都必须将 CA 的公钥存放在本地。为了保持 Internet 上的通用性,目前一般的 SSL 协议实现只要求服务器方向客户方出示证书以证明自己的身份,而不要求用户方同样出示证书,在建立起 SSL 信道后再加密传输用户的口令,实现客户方的身份鉴别。

同网络层安全机制相比,传输层安全机制的主要优点是它提供基于进程对进程的(而不是主机对主机的)安全服务和加密传输信道,利用公钥体系进行身份鉴别,安全强度高,支持用户选择的加密算法。这一成就如果再加上应用级的安全服务,就可以提供更加可靠的安全性能了。

7.9 DNS 风险及缓解方法

7.9.1 直接风险

Internet 中的 DNS 协议是不安全的。DNS 安全的前提是假定 DNS 服务器之间是可信的，即 DNS 系统假定 DNS 服务器不会故意提供错误的信息。DNS 协议不提供客户和服务器之间的身份鉴别，这就使攻击者可破坏这种可信关系。

DNS 攻击包括无身份鉴别的响应，缓存受损以及 ID 的盲目攻击。此外某些 DNS 的实施易破坏 DNS 分组。

1. 无身份鉴别的响应

DNS 使用一个会话标识来匹配请求和回答，但会话标识不提供身份鉴别。攻击者观察 DNS 请求，能伪造一个 DNS 回答。假的回答会有观察到的会话标识。结果是一个未经身份鉴别的响应看起来似乎是已鉴别的。攻击者甚至可在分组中设置授权的标记，去除对数据正确性的怀疑。请求者接到回答和接受未经身份鉴别的响应，结果是攻击者能控制主机名的查找，并进一步重指被害者的连接，如图 7-3 所示。

2. DNS 缓存受损

任何地方有未经身份鉴别的响应针对请求者，就能针对任何类型的 DNS 服务器缓存，使 DNS 缓存受损。攻击者观察 DNS 请求，并生成一个伪造的 DNS 回答。回答看来似乎是授权的，且含有一个长的缓存超时值。受损的 DNS 服务器可对任何数据请求提供假数据。这就使请求者的域不可达。而且会一直提供错误的信息，只要受损信息在缓存中。

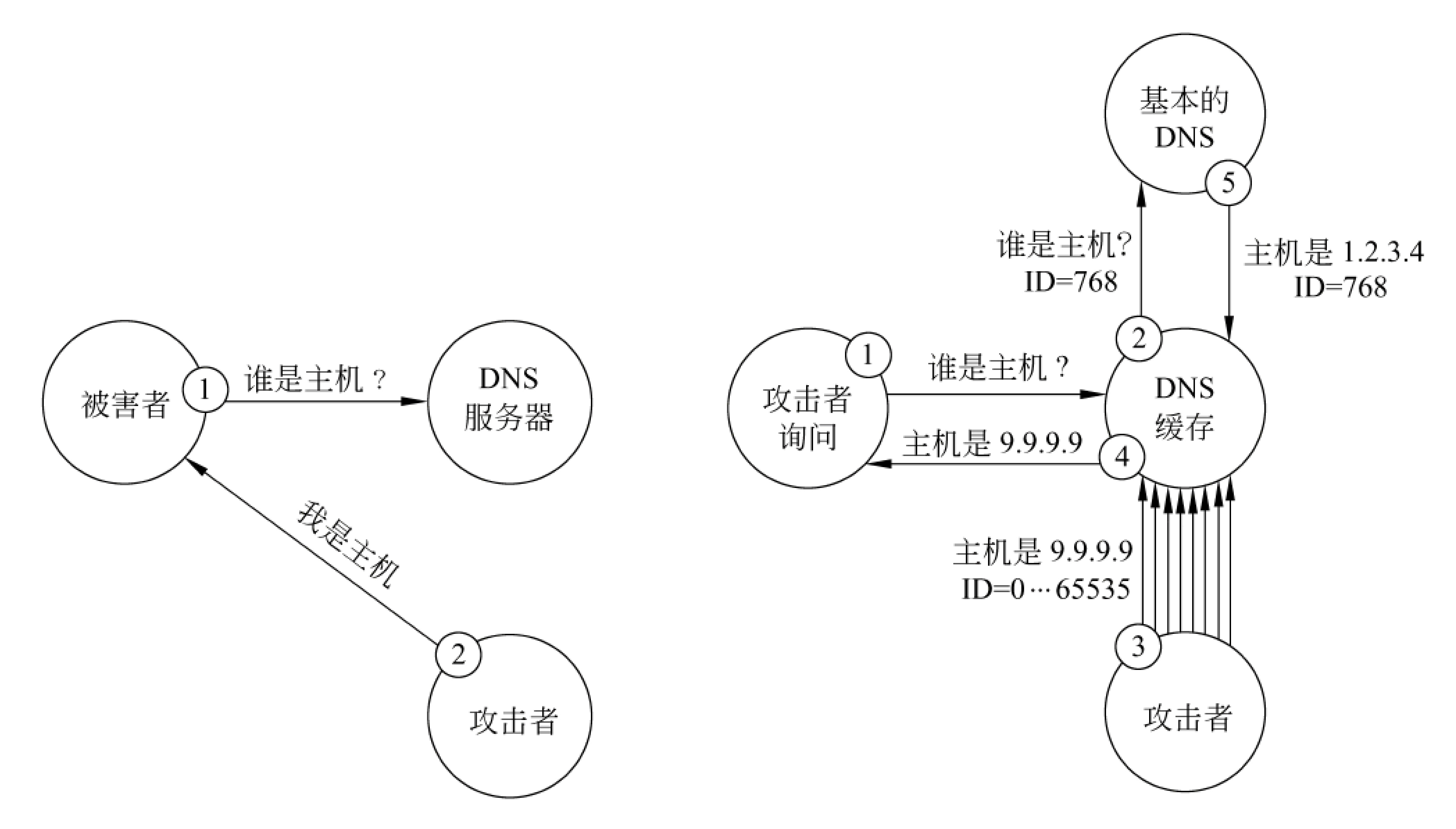


图 7-3　未经身份鉴别的 DNS 响应攻击

图 7-4　ID 盲目攻击

3. ID盲目攻击

未经鉴别的响应和缓存受损都需要攻击者观察到 DNS 请求和会话标识。但观察一个请求不总是必需的。当主机名出现超时,攻击者可选择一个通用的域名,并开始攻击。攻击的方法是生成 DNS 回答的泛滥,每个回答包含一个不同的会话标识,如图 7-4 所示。

4. 破坏 DNS 分组

DNS 协议规定了查询和回答的数据大小。但某些 DNS 实施没有适当地检查数据边界。分组可声称含有比实际更多的数据,或没有包含足够的数据。其结果是缓冲器溢出和不足。

7.9.2 技术风险

直接的 DNS 风险是由于协议本身的影响,但技术风险是基于配置的问题。影响和修改 DNS 服务器数据的能力直接导致 DNS 遭破坏。技术风险包括 DNS 域拦截、服务器拦截、更新持续时间以及动态 DNS。

1. DNS 域拦截

任何 DNS 服务器的所有者能把服务器配置为任何域的一级源。DNS 并不包含域所有者的概念。假如一公司要配置其内部服务器为 microsoft. com 域的一级源,无法阻止它这样做。但 DNS 的层次结构能阻止这类配置作为无效信息在 Internet 中泛滥。假如 DNS 服务器在服务器链中级别足够高(也就是 SLD,ccTLD 或大的服务提供者的缓存服务器),那么,它就能拦截全部域。

DNS 拦截是可行的,很多计算机蠕虫、病毒、间谍软件以及很多恶意软件将信息送到 Internet 的远程主机。最通用的阻止这些风险的缓解方法是使恶意软件不能搜集主机。假如主机是不可达的,那么它就不能收集信息。当恶意软件站点的 IP 地址被设定,防火墙的出口过滤能阻止用户访问。当恶意软件用名字来访问远程主机,DNS 成为最佳的过滤选择。本地 DNS 服务器能配置成可阻止恶意软件站点对主机名的查找。假如主机名不能查找到 IP 地址,那么,主机不可达。

利用 DNS 服务器来阻断不希望的主机名查找能阻断访问不希望的站点,在这些站点的主机服务同色情、欺骗和恶意软件有关。很多站点用过滤的方法免除在线风险。

2. DNS 服务器拦截

DNS 服务器能被拦截。被拦截的服务器能配置成提供不同的主机信息或包含一些新的主机名。DNS 拦截通常发生的两种情况,即系统被破坏或 IP 拦截。

DNS 服务器作为应用程序在计算机上运行。假如攻击者能访问计算机系统,那么攻击者就能访问 DNS 服务器。只要主机系统存在潜在的遭破坏的风险,那么 DNS 服务器也是易受损的。例如,在主机上运行着一台老的打印服务器,后者又易于被远程利用而受破坏,那么 DNS 服务器也会因这种远程利用而易受破坏。

为了缓解系统被破坏的风险,关键的 DNS 服务器应运行在加固的系统。加固的系统对所有不必要的服务不予以提供。

DNS 是一个高层协议，这意味着它对所有低层风险是易于受破坏的。因为大部分 DNS 服务器运行在 IP 上的 UDP 或 TCP，而 IP 拦截或 ARP 拦截是容易的。假如攻击者能拦截 IP 或 ARP 分组，那么攻击者就能假冒 DNS 服务器。虽然这种类型的 DNS 拦截十分少见，却是十分危险的。

3. 更新持续时间

缓存 DNS 服务器同每个 DNS 项的超时相关联。当主机配置改变时，超时防止数据失效。假如超时值太大，则不能立即完成改变。假如管理者立即重新定位主机，那么缓存服务器将指向错误的地址。

4. 动态 DNS

动态主机配置协议 DHCP 普遍用于对本地网上的主机分配网络信息。DHCP 提供带有网络地址的新的主机、默认的网关以及 DNS 服务器信息。这些主机只能用它们的网络地址访问，用户不能用主机名来访问。动态 DNS(DDNS)解决 DHCP 的主机名问题。使用 DDNS，DHCP 的客户能在本地 DNS 系统放主机名。虽然 DHCP 客户每次被分配一个新的连到网络的网络地址，但是 DDNS 确保主机名总是指到主机的新的网络地址。

客户能很容易地配置 DDNS 主机名，但是 DDNS 允许名字拦截。任何不和活动 DHCP 地址相联系的主机名都可被请求。假如一台主机是离线的或不可用，那么，另一台主机能容易地拦截该主机名。只要被拦截的名字同有效的 DHCP 主机相联系着，真正的主机就不能请求该名字。

7.9.3 社会风险

DNS 在 Internet 中扮演了一个关键的角色。破坏和拦截主机名直接导致 DoS，MitM 以及其他系统攻击。DNS 服务器除了有直接风险和技术攻击风险外，还有其他一些破坏主机和域的方法。这些风险来自人为因素，归结为 DNS 社会风险，包括相似的主机名、自动名字实现、社会工程以及域的更新。

1. 相似的主机名

当使用键盘时，打印错误是经常的，这样造成用户常常输入一个错误的主机名。攻击者能利用这些知识拦截连接。例如用户要连接到北京银行 Bank of Beijing，其域名是 bankofbeijing.com.cn，用户可能不经意地将其域名输入为 bonkofbeijing.com.cn。假如攻击者有相似的主机名，那么，就可伪装成真实的站点，并攻击用户的连接。

2 自动名字实现

很多 Web 浏览器支持自动名字实现，用户可不输入域名服务器的最高级域名(即 .com)，而只输入主机名的中间部分。自动名字实现可附加一串后缀，直至找到主机名。通常最先试的后缀是.com。假如 Web 站点不是以.com 结尾，那么，攻击者能注册.com 名字来有效地拦截这个域。

一个著名的名字自动实现拦截的例子是发生在 1997 年对美国白宫网站 whitehouse.gov 的拦截。攻击者注册了一个 whitehouse.com 的色情网站。用户在其浏览器输入

whitehouse,自动名字实现引导该用户进入该色情网站,而不是白宫总统的网站。

3. 社会工程

社会工程是描述社会学信念的术语。社会工程不是用计算机来破坏一个系统,而是用伪装和一般技术。可以使用电子邮件或电话来改变授权者,并取得所需的信息。

域名注册是通过少数域名注册机构。如果注册机构被说服,该用户是该域名的授权拥有者,那么,域名信息就可修改或转换。

4. 域更新

域名注册机构并非无限期地赋予域,而是有限期的。超期后该域名就放弃。通常注册域的期限为一两年或五年。假如域主没有注意过期,忘了去更新域名。当过期后,任何人可注册相同的域名。这就使攻击者能故意侵占一个域名,并伪装成该组织。

7.9.4 缓解风险的方法

DNS 的设计是用来管理大量的网络地址信息。设计时考虑了速度、灵活性和可扩展性,但并未考虑其安全问题。它并不提供身份鉴别机制,且假定所有的询问是可信的。有几种缓解 DNS 风险的方法。使 DNS 安全的主要方案是基于特定的服务器配置、可信的定义以及其他一些解决方案。

大部分 DNS 风险缓解方法基于模糊安全和打补丁。基本的预防方法包括直接的、技术的、侦察以及社会威胁的缓解。

1. 直接威胁缓解

基本的维护和网络分段能限制直接威胁的影响。

- 补丁:DNS 服务器的增强版经常会发布,DNS 服务器和主机平台应定期打补丁和维护。
- 内部和外部域分开:DNS 服务器应该是分开的。大的网络应考虑在内部网络分段间分开设置服务器,以限制单个服务器破坏的影响,且能够平衡 DNS 负载。
- 限制域的转换:域的转换限制于特定的主机,且由网络地址或硬件地址标识。这个方案对 MAC 和 IP 伪装攻击是脆弱的,但对任意的主机请求域转换确实是有用的。
- 鉴别的域转换:采用数字签名和鉴别域转换能减少来自域转换拦截和破坏的影响。
- 有限的缓冲间隔:缓冲间隔减少至低于 DNS 回答规定的值,可以减少缓冲器受损的损坏窗口。
- 拒绝不匹配的回答:假如缓冲 DNS 服务器接到多个具有不同值的回答,全部缓冲器应刷新。虽然这会影响缓冲器性能,但它消除了长期缓冲器受损的风险。

2. 技术威胁的缓解

技术风险预防方法包括网络、主机和本地环境。

- 加固服务器:限制远程可访问进程的数量,就能限制潜在攻击的数量。加固服务

器可降低来自技术攻击的威胁。

- 防火墙：在 DNS 服务器前放置硬件防火墙限制了远程攻击的数量。

3. 侦察威胁的缓解

- 限制提供 DNS 信息：这可以缓解攻击者侦察的威胁。虽然 DNS 不能完全做到，但可限制提供信息的类型和数量。
- 限制域转换：域的转换仅限于鉴别过的主机。虽然不能阻止蛮力主机的查找，但可阻止侦察。
- 限制请求：限制 DNS 请求的数量可由任何单个网络地址完成。虽然不能防止蛮力域监听，但可设置障碍。
- 去除反向查找：假如反向查找不是必需的，那么去除它。这可限制蛮力域监听的影响。
- 分开内部和外部域：DNS 服务器应该是分开的，以确保 LAN 的信息保持在 LAN。特别是内部主机名应该不允许外部可观察。
- 去除额外信息：不是直接为外部用户使用的信息应该去除，例如 TXT，CNAME，HINFO 这些信息。
- 隐藏版本：对允许本地登录或远程状态报告的 DNS 服务器，这些 DNS 版本可能被泄露。因为不同的版本和不同的利用相关，应该修改版本以报告假信息或将其去除。

4. 社会威胁缓解

除了对用户进行培训，防止相似主机名和自动名字完成的风险，还有以下一些：

- 监控相似域：经常搜索域名的变化。当发现有相似主机名的标识，DNS 提供者要求他们关掉。虽然这是一个复杂的耗时的任务，但这是监控相似域名的一种专门服务。
- 锁住域：使用支持域锁定的域注册者。这需要一些附加信息，诸如账户信息、转换域名的口令。
- 使用有效联系：在域注册中提供一个或多个有效联系方法，以允许用户和注册者联系域主。但不需要专门的人名或个人信息，以免攻击者使用这些信息攻击域主。
- 不间断支持：选择一天 24 小时，一周 7 天不间断支持的域注册者。这样在任何时候可和注册者联系，以解决有关域的问题。
- 自己主持：大的单位应选择成为拥有管理自己域的注册者。

5. 优化 DNS 配置

绑定(BIND)是通用的 DNS 服务器实施。有很多文本专门描述如何绑定 DNS 服务器的配置方法。有些文本还包括安全绑定，即如何防止 DNS 服务器被拦截。Internet 安全联盟提供了很多配置安全 BIND 的资源。

6. 确定可信的回答

一般 DNS 服务器不提供可信的标记，DNS 客户端无法决定回答是否是合法的。

DNS 安全扩展(DNSSEC)提供签名以鉴别信息以及对每个回答响应的数字标记。然而,DNSSEC 在使用前需要发鉴别钥,但它只鉴别服务器而不对内容鉴别。

更为通用的方法是用两个 DNS 服务器,一个用于 LAN,另一个用于 WAN。LAN 服务器对所有内部主机提供 DNS 支持。这可防止外部黑客的破坏。WAN 的 DNS 服务器对外部主机提供信息。

7.10　SMTP 邮件风险

SMTP 邮件系统在当初设计时,主要考虑可靠地、及时地传递报文,并没有考虑安全。这就导致 SMTP 的一系列安全风险。

1. 伪装报头及垃圾邮件

邮件用户代理 MUA 能指定邮件报头,每个邮件中继附加接收到的报头到邮件的开头。这些报头用来跟踪报文。

伪装的邮件报头发生在发送者故意插入假的报头信息。正常的邮件用户代理 MUA 和邮件传送代理 MTA 系统只加有效的报头,但恶意的系统有可能加上假的信息,去除合法的报头,或修改存在的报头。要区别有效报头和无效报头是很困难的。

除了最后接收的报头以外,电子邮件报头的所有属性都可以伪造。主题、日期、接收者、内容甚至最初接收的报头都能用 SMTP 数据命令来伪造。当电子邮件送到一个真实的 MTA,有效的接收报头加到报文的前面,包含一个有效的时间戳和原始的 IP 地址。

伪装的电子邮件能导致十分严重的后果,包括对一个组织的信誉。垃圾邮件也是伪造电子邮件滥用的例子。据统计垃圾邮件占整个电子邮件的 80%,垃圾邮件如此多的原因一方面是因为缺乏身份鉴别,另一方面是因为造成伪装报头只需要很低的技巧。反垃圾邮件的解决方法主要是过滤和拦截大约 90%垃圾邮件。但垃圾邮件制造者不断改换使用的技术,以致使静态反垃圾邮件系统失效。过滤不仅针对垃圾邮件,也会不经意地误把非垃圾邮件也过滤掉。

识别伪装的电子邮件需要把有效电子邮件和伪装电子邮件区分开来,但这是十分困难的。一般来说,一个伪装报头预示在它后面的信息都是伪造的。但是某些域是能确定的。接收的报头应包含“from”和“by”地址。一个报头“by”地址应该和下一个报头的“form”地址相匹配。大部分伪装的接收的报头并不把“from”和“by”地址合适的相连。接收的报头应包含一个时间戳和跟踪号。假如这些不存在,或产生很大延迟,那么,该报头似乎是伪造的。

大部分可观察的属性来自发送者及其内容。假如发送者是不认识的,内容是不希望的,那么,该电子邮件似乎不是要求的,报头大概是伪造的。

大部分电子邮件服务器保持处理日志。加到接收报头的唯一识别符应和 MTA 生成的日志条目匹配。当跟踪一个电子邮件,邮件日志能帮助判定真的源。日志通常包含发送者、接收者、时间戳、IP 地址,甚至进程的识别。当伪造电子邮件,服务器列出的假的报头没有日志条目。

虽然邮件日志能用来跟踪电子邮件,但并非总是可取的。因为来自不同的服务器的日志经常是不可访问的,对匿名系统也是不可取的。

2. 中继和拦截

SMTP 并非总是将电子邮件从发送者直接送到接收者,通常使用邮件中继来路由信息。结果是主机可以是一个中继。邮件中继是由 DNS 中的 MX 记录来决定的。

SMTP 管理员无须专门的允许来操作中继,而且电子邮件通常是用明文传送。结果是中继的拥有者能读电子邮件,每个电子邮件中继有可能拦截或修改报文的内容。

为了缓解拦截的风险,敏感的电子邮件使用内容加密。PGP 是常用的加密电子邮件的例子(RFC 2440)。但是加密技术用于电子邮件有其局限性:

- 兼容性:并非每个电子邮件加密实施都是遵从标准。例如,PGP 用 mutt(UNIX 邮件客户)加密的电子邮件,对用 Microsoft Outlook(PGP 支持的)用户不是很容易能看到的。愈是复杂的加密系统愈安全,但和其他电子邮件系统的兼容性愈差。
- 一致性:电子邮件最大的强项是能发送报文给任何人,甚至完全陌生的人。流行的密码系统需要发送者对接收者有事先的了解,包括交换密钥。

3. SMTP 和 DNS

SMTP 最大的风险来自于它对 DNS 的依从。DNS 用来识别邮件中继,然而 DNS 对很多形式的攻击特别容易受破坏。结果是电子邮件通过 DNS 也受损。电子邮件可路由到敌意的中继或单纯地被阻断。

4. 低层协议

如同 SMTP 受到 DNS 破坏的影响,SMTP 也会受到低层协议,诸如 MAC,IP 和 TCP 拦截的影响,破坏正在传送的电子邮件。因为 SMTP 不提供数据内容加密,任何攻击者沿着网络通路能看到所有通过的电子邮件。

一般来说,假如安全是主要的考虑因素,那就不应使用电子邮件。特别是明文的电子邮件不应用来传送口令、信用卡信息或保密信息。

5. E-mail 的伦理问题

问题不仅在于技术上的限制,诸如鉴别、拦截和报头伪装,还有由于所有权和分发引起的伦理和法律问题,包括拷贝权和个人隐私等问题。

首先是 E-mail 的处理和使用,没有任何技术因素使接收者不能转发电子邮件给其他人,即使邮件上标志“保密”、“分类”,仍能分发出去。有些组织制定 E-mail 管理政策和使用E-mail 规则,但从技术上无法阻止违规行为。

E-mail 的伪装是另一类问题。最简单的伪装方法只需配置一个带有别人 E-mail 地址的邮件客户 MUA,更复杂一点的伪装使用自动工具,通过代理中继和 MTA 通信,提供精致的伪装报头。

E-mail 只是提供一个简单的从发送者到接收者的通路,SMTP 无法验证电子邮件的传送以及电子邮件是否已被接收者接收。为此 SMTP 可扩展其功能,包括传递通知,采用回执和投递通知两种方法。但是这两种方法都无法证明接收者是否确实收到了该邮

件，都有可能被中间结点收到。

7.11　HTTP 风险

HTTP 的设计目标是灵活和实时地传送文件，没有考虑安全的因素。但是使用 HTTP 的各种应用都期望提供身份鉴别、认证和隐私。这就导致基于无身份鉴别 HTTP 系统的风险。此外 HTTP 服务器的配置和 CGI 的各种应用能对远程攻击暴露系统。

HTTP 使用通用资源访问地址 URL 作为定义查询类型的缩写标记。它不仅允许标识远程服务和文件，而且也导致暴露攻击的目标。

7.11.1　URL 漏洞

URL 为用户提供了方便识别网络资源的方法，URL 可识别服务、服务器以及资源参数。攻击者能策划一个敌意的 URL 并把被害者指向另一个位置，导致被破坏。有很多攻击 URL 的方法，比较常用的方法有主机名求解攻击、主机名伪装、剪切和拼接以及滥用询问。

1. 主机名求解攻击

URLs 通常用主机名到基准服务器，这使用户容易记住不同的文本字符串，而无须用不易记忆的网络地址。假如攻击者能重置主机名求解系统，那么查询能送至另外的服务器。这能构成 MitM、伪装或 DoS 攻击。

前面曾讨论过破坏 DNS 的各种方法。对 URLs 来说，诸如相似的主机名和自动完成这类社会风险比直接 DNS 破坏更加通用。

2. 主机伪装

有一些伪装主机名的方法，而无须修改主机名求解系统。例如网络地址能用整数表示，有一些不常用的工具能把整数转换成网络地址，但很少常规的 Web 用户使用这种过渡的技术工具，让主机名在 URL 中，甚至很少计算机用户能识别它。因此网络地址的整数伪装是十分成功的。

另一种伪装方法是使用主机名域在 URL 中。大部分 Web 服务器无须基于 URL 的鉴别，因此用户名和口令域是被忽略的。攻击者能在用户名中插入一个假定用户不会注意到的主机名。钓鱼以及其他伪装攻击通常使用这种伪装形式。

3. 统一资源标识符(URI)伪装

URI 用来描述资源和参数，但并非所有字符都是有效的。例如 HTTP 询问使用间隔符命令、URI 和版本信息隔开，URI 不能包含间隔。为了描述更大的字符集，URI 字符能用百分率符号和 ASCII 字符编码。

攻击者能用 URI 编码来伪装主机名和 URI 信息。类似地，URI 内的字符也能伪装，以阻止大部分用户明白 URI 的内容。

4. 剪切和拼接

URL 对远程资源定义一个逻辑通路。该通路容易被修改,其中最通用的两个修改方法是剪切和拼接。

剪切只需简单地移掉 URI 一部分成分。虽然安全服务器对该操作将返回或给出 404 差错。但对很多服务器仍能被浏览,以致一些私人的 Web 页面能被看到。

和剪切相反,拼接是附加一些信息至 URL。例如大部分 Apache Web 服务器有 images 和 icons 目录。在原来的 URI 拼接上 icons 后,即使不能打开其目录,但返回码的类型能确定该 icon 目录是否存在。即使不能访问该资源,不同的返回差错信息也能确认资源是否存在。为此应加固 HTTP 服务器,加固的方法包括:

- 假如不需要的话,一些默认的目录应去掉。
- 开放的目录应关掉。
- 访问允许差错和文件没有找到差错的默认回答应相同。攻击者应不能识别服务器上的私人资源。
- 私人的和临时的文件应不放在公共服务器上。
- 内容不能看的目录和文件应从公共服务器去除。

5. 滥用查询

什么地方有剪切和拼接修改 URI 的通路,那么,存储在 URI 的选项就能被修改。大部分包括选项的 URL 是 CGI 应用,CGI 是通过网关接口,用来和 HTTP 服务器的应用来接口。它允许服务器传递动态内容,而不仅是静态 Web 页面。URI 选项经常用来控制 CGI 功能。

大部分 URI 选项的格式是 field=value。改变这些参数值能导致改变应用功能,可以导致侦察和开发漏洞。例如攻击者能识别参数值的范围和不同的响应码,从而更加详细地了解系统。在某些情况,参数值可以是其他 URL 或文件通路,从而获得 HTTP 服务器通常使用权的信息访问。当参数用来存储状态信息,攻击能修改参数值,就有可能访问用于其他用户的信息。为了缓解修改选项的风险,CGI 应该验证所有的参数。

6. SQL 插入

SQL 是结构化查询语言,用来访问数据库信息。SQL 插入攻击是通过修改 SQL 命令,使提交到 URL 的参数和选项直接送到数据库查询。通过使用未检验的输入,攻击者能修改查询请求。

例如下面是一个 SQL 查询:

```
SELECT login,password,name
FROM accounts
WHERE login='$ LOGIN';
```

URL 可使用 http://server/cgi-bin/account? login = bob 来访问,这里可设置 $LOGIN 的值为 bob。但一个敌意的用户可以提交一个 URI 如下:

```
/cgi-bin/account?login='bob';+INSERT+INTO+accounts+('evil','pass','Eiil User');commit;1='x'
```

这样经 URL 扩展后,SQL 查询如下:

```
SELECT login,password,name
FROM accounts
WHERE login='bob';
INSERT INTO accounts('evil','pass','Eiil User');
commit;
1='x';
```

在 URI 中的单引号允许完成 SQL 查询,附加的值成为使用的 SQL 语句。这个例子插入了一个新的账户,该账户带有 login evil 和 password pass。使用这个攻击形式,攻击者能选择变更的数据,插入新的数据,删除存在的数据,生成新的表或删除已有的表。任何 SQL 服务器可用的功能都能被攻击者访问。

为了缓解 SQL 插入攻击有以下几种方法:

- 所有由 HTTP 客户送来的参数必须加单引号,因此它们不会扩展成可执行的语句。
- 所有输入的参数在使用前必须验证。不安全的字符,诸如单引号、双引号、型式匹配字符应该加上单引号,移去或无保留地拒绝。
- 使用查找表,而不是直接使用客户提供的表信息。例如,不用 table=account,客户能定义 table=1,在 CGI 中的查找表将 1 转换到 account,以阻止攻击者定义任意的数据库表。
- 数据库的差错信息不应传给最终用户,应传给 CGI 应用程序,并将其转换成有用的用户级信息。如果将数据库差错信息直接提供给用户,只能帮助攻击者,导致进一步的 SQL 插入攻击。

7. 跨站脚本

跨站脚本 XSS(Cross-Site Scripting)攻击发生在当用户把数据提交给服务器后,又被送到另一用户。例如很多在线论坛和博客允许用户张贴内容和超级链接。张贴的东西立即可被其他用户访问。例如攻击者张贴敌意的 Java Script,Java 或可执行的病毒,那么,其他用户通过 XSS 攻击指向而受到影响。

虽然传送活动码(诸如 Java Script 或病毒)能导致直接攻击,但一些不活动的攻击可包含到敌意站点或假信息的链路。

为了缓解 XSS 攻击的风险,用户张贴的信息应该是受审查的。HTML 和活动成分应审计和过滤。很多基于 Web 的论坛不允许包括 HTML 内容的传送,或严格地限制 HTML 成分。如可能的话,张贴公共发布信息前应予以评估。

7.11.2　常见的 HTTP 风险

如上所述,HTTP 的设计没有考虑安全的因素,而使用 HTTP 的各种应用却期望提供鉴别、认证和隐私,这导致基于无鉴别的 HTTP 系统的各种风险,常见的 HTTP 风险有以下几种。

1. 无身份鉴别的客户

HTTP 并没有提供很多方法为服务器对 HTTP 客户端的身份进行鉴别。一些基本的鉴别方法广泛被使用，传输的凭证并不提供保密。因为用明文传输数据，像 Telnet 和 FTP 用的基本身份鉴别是不安全的。虽然可以用 SSH 来替代 Telnet 和 FTP，但 SSH 的连接速率很慢，因此很少用它来替代 HTTP。其他 HTTP 鉴别系统（诸如摘要身份鉴别）很少被支持，而且摘要是用明文传输的，易受字典攻击的破坏。

带有客户端证书的 HTTP 可提供客户端的身份鉴别，但很少系统使用客户端证书，再加上 SSL 也有基于身份鉴别的一系列风险。然而，在 HTTP 上使用基本的身份鉴别或摘要身份鉴别对提供身份鉴别或隐私是足够的。一般而言，很少 HTTP 系统对客户端进行身份鉴别。

2. 无身份鉴别的服务器

如同客户端无身份鉴别，服务器也常常无身份鉴别。客户端依据主机名或网络地址作为对服务器的识别。主机名识别易受 DNS 攻击的损害，网络地址易受网络拦截的破坏。虽然 SSL 提供某些验证，但浏览器的使用问题常常阻止用户有效地使用验证的系统。没有客户端和服务器的证书，SSL 只能提供有限的身份鉴别支持。

3. 客户端隐私

通常 HTTP 运行在一个独立的环境，每个 HTTP 请求是独立的。Cookies 和身份鉴别系统可跟踪用户，但只是限制在特定的服务器。然而 HTTP 报头提供交叉服务器跟踪。Web 浏览器提供参考报头并指示链接的 URL 来自何处。

参考报头用于 Web 站点收集访问者的统计信息。跟踪这个信息，一个站点可识别哪些别的站点和它相连。

但是参考报头包括整个 URL，如果参考 URL 包含查询选项，那么目标服务器能识别正在查询的项目。假如参考 URL 包含登录凭证，那么目标服务器能收到这些凭证。

4. 信息泄露

大部分 HTTP 客户端和服务器泄露大量信息。HTTP 请求报头通常泄露 Web 浏览器的类型，包括版本及操作系统。类似地，HTTP 回答报头常常包含服务器类型、版本以及支持的插入（plug-in）。虽然服务器可以加固以隐蔽信息，但 CGI 应用常常基于浏览器类型（用户代理）来修改回答。加固的浏览器发送没有鉴别的信息，可能阻断访问服务器。

从 HTTP 回答的信息包括一个时间戳。时间戳通常是一个文件最近的修改时间，而 CGI 应用通常返回当前的时间。通过观察时间戳，攻击者能识别数据是静态的（来自文件）还是动态的（来自应用程序）。此外，静态的时间戳能泄露最近的修改时间。老的文件表明目录很少被监控，而每天或每周修改的文件表明管理者或自动脚本何时访问该系统。攻击者能利用这个时间戳来策划攻击。

5. 服务器定位轮廓

虽然 IP 地址可用来将服务器限定到特定的区域、国家或城市，但很多大的公司的子网分布在很多国家。可利用 HTTP 泄露的信息来定位服务器的地理位置，这些泄露的信息包

括 HTTP 的时区和 HTML 的本地语言,都可以用来确定服务器所在的国家或地区。知道了服务器所在的国家和位置有利于攻击者确定攻击时间,以避开服务器管理者监控的时间。

为了缓解服务器定位轮廓的风险,要尽量减少时间、地理位置和语言信息的泄露。很多 Web 应用程序不用本地时间,而用 Web 用户的相对时间。高敏感系统应不泄露时区和本地语言信息,或配置成变换的时区和默认的语言设置。使用格林威治时间 GMT 配置系统能阻止定位轮廓。

6. 访问操作系统

OSI 应用层直接和主机操作系统接口。通过访问文件或应用程序(经 CGI 程序),HTTP 服务器提供直接访问来处理 HTTP 命令。通过修改 URL 通路和选项,针对操作系统的漏洞可被远程访问。

不管什么应用,HTTP 服务器需要直接的系统访问。暴露的问题只是访问系统的自由度。甚至于开放目录或文件时间戳也能用于攻击前的侦察。

7. 不安全的应用程序

虽然隐私问题、XSS、开放目录以及信息泄露能导致攻击目标,但是不安全的 CGI 应用程序形成最大风险。通过专门的编程可以缓解应用程序的风险。加固 Web 服务器本身也可减少这类风险。开放 Web 应用安全项目 OWASP(The Open Application Security Project)提供了详细的列表对 Web 服务器进行安全预防,包括身份鉴别、授权、会话以及隐私管理。

8. 低层协议

HTTP 漏洞风险也来自低层协议。DNS 攻击、TCP 拦截和更低层的攻击也能阻挡 HTTP、拦截信息或拦截连接。即使带有 SSL 和摘要鉴别,HTTP 仍然会受到端点攻击的威胁。例如攻击者可以利用有效凭证建立一个 SSL 连接和鉴别,然后企图攻击 CGI 应用程序。

7.12 本章小结

不同类型的漏洞、攻击和威胁存在于 Internet 的不同层次,Internet 安全体系结构就是对于不同类型的攻击实施不同层的保护。本章重点分析传输层和应用层的风险以及缓解风险的方法。

传输层的主要风险围绕着序列号和端口。要拦截传输层连接,攻击者必须破坏分组序列。传输层端口直接导致网络服务,目标瞄准端口,远程攻击者可针对一个专门的高层服务。传输层还能导致侦察攻击,包括端口扫描和信息泄露。

TCP 侦察、TCP 拦截、TCP DoS 都是对 TCP 的攻击方法,缓解对 TCP 攻击的方法有改变系统框架、入侵检测和入侵防御等。

由于 TCP/IP 协议本身非常简单,没有加密、身份鉴别等安全特性,因此要向上层应用提供安全通信的机制就必须在 TCP 之上建立一个安全通信层次。最常用的是传输层套接字层 SSL,它的主要优点是它提供基于进程对进程的(而不是主机对主机的)安全服

务和加密传输信道。

Internet 中的 DNS 协议是不安全的，它不提供客户和服务器之间的身份鉴别。DNS 风险包括直接风险、技术风险和社会风险。大部分 DNS 风险缓解方法基于模糊安全和打补丁，基本的预防方法有直接的、技术的和社会的威胁缓解以及优化 DNS 配置等。

SMTP 邮件风险包括伪装报头、垃圾邮件、中继和拦截等。SMTP 邮件最大的风险是对 DNS 的依从，它也会受到低层协议诸如 MAC，IP 和 TCP 拦截的影响。SMTP 邮件还有伦理和法律的问题。PGP 是常用的加密电子邮件，以缓解风险的方法。

常见的 HTTP 的风险包括 URL 漏洞、无身份鉴别的客户、无身份鉴别的服务器、客户端隐私、信息泄露、服务器定位，以及不安全的应用程序等。OWASP 是缓解 HTTP 风险的一种有效方法。

习　　题

1. 传输层有哪些风险？试比较一个端口和多个端口以及静态端口和动态端口的风险。
2. 哪些 TCP 信息的类型可用来识别操作系统框架？
3. 假如客户到服务器的连接被拦截，会引起什么后果？
4. 列出 5 种方法来缓解 TCP 攻击的威胁。
5. 什么技术可用来减少 IP，TCP 和 UDP 的攻击指向？
6. DNS 协议是不安全的，它存在哪些安全风险？有哪些缓解这类风险的方法？
7. 哪些风险是由于 DNS 配置不当引起的？有哪些缓解这类风险的方法？
8. 哪些方法可缓解对 DNS 的侦察威胁？
9. 什么是 SMTP 通信的四类直接威胁？
10. 哪些是攻击 URL 的方法？
11. 常见的 HTTP 风险有哪些？
12. HTTP 客户端和服务器通常会泄露哪些信息？
13. SSL 产生会话密钥的方式是什么？
14. 传输层保护的网络采用的主要技术是建立在什么基础上的？

第 3 篇
网络安全技术

第8章 防 火 墙

本章要点：

- 防火墙原理；
- 防火墙主要技术；
- 防火墙体系结构；
- 堡垒主机的作用及部署；
- 数据包过滤规则；
- 状态检测数据包过滤原理。

8.1 防火墙的原理

8.1.1 防火墙的概念

防火墙是建立在内外网络边界上的过滤封锁机制，内部网络被认为是安全和可信赖的，而外部网络(通常是 Internet)被认为是不安全和不可信赖的。防火墙的作用是防止不希望的、未经授权的通信进出被保护的内部网络，通过边界控制强化内部网络的安全政策。防火墙在网络中的位置如图 8-1 所示。

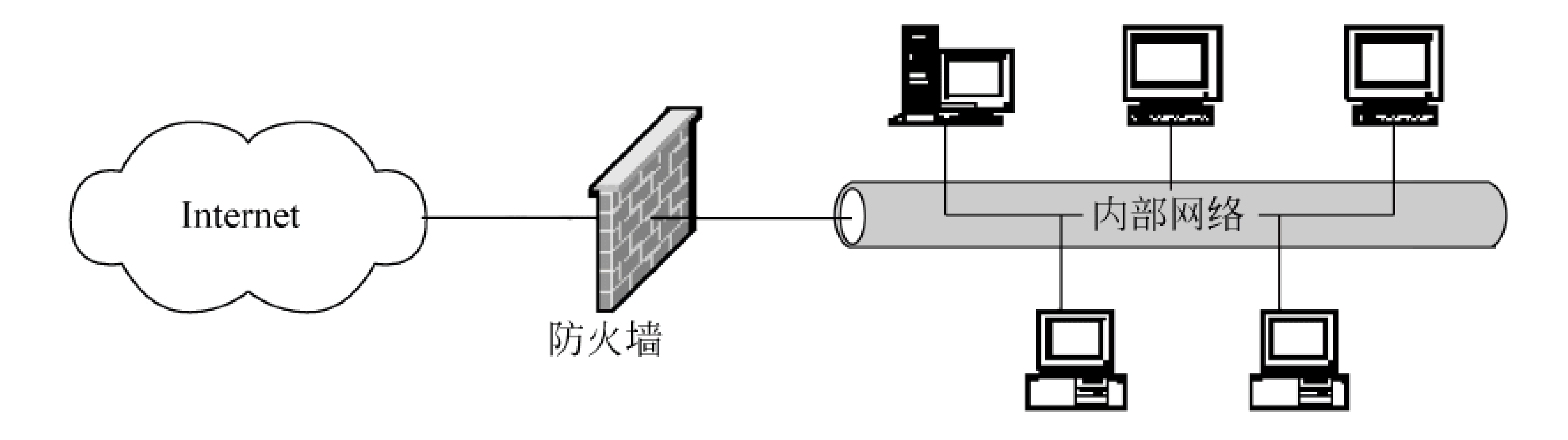


图 8-1　防火墙在网络中的位置

防火墙通常是运行在一台或者多台计算机之上的一组特别的服务软件，用于对网络进行防护和通信控制。但是在很多情况下防火墙以专门的硬件形式出现，这种硬件也被称为防火墙，它是安装了防火墙软件，并针对安全防护进行了专门设计的网络设备，本质上还是软件在进行控制。

如果没有防火墙，则整个内部网络的安全性完全依赖于每个主机，因此，所有的主机都必须共同达到一致的高度安全水平。也就是说，网络的安全水平是由最低的那个安全水平的主机决定的，这就是所谓的“木桶原理”，木桶能装多少水由最低的地方决定。网络

越大，对主机进行管理使它们达到统一的安全级别水平就越不容易。

防火墙隔离了内部网络和外部网络，它被设计为只运行专用的访问控制软件的设备，而没有其他的服务，因此也就意味着相对少一些缺陷和安全漏洞。此外，防火墙也改进了登录和监测功能，从而可以进行专用的管理。如果采用了防火墙，内部网络中的主机将不再直接暴露给来自 Internet 的攻击。因此，对整个内部网络的主机的安全管理就变成了防火墙的安全管理，这样就使安全管理变得更为方便，易于控制，也会使内部网络更加安全。

防火墙一般安放在被保护网络的边界，必须做到以下几点，才能使防火墙起到安全防护的作用：

(1) 所有进出被保护网络的通信必须通过防火墙。

(2) 所有通过防火墙的通信必须经过安全策略的过滤或者防火墙的授权。

(3) 防火墙本身是不可被侵入的。

总之，防火墙是在被保护网络和非信任网络之间进行访问控制的一个或者一组访问控制部件。防火墙是一种逻辑隔离部件，而不是物理隔离部件，它所遵循的原则是，在保证网络畅通的情况下，尽可能地保证内部网络的安全。防火墙是在已经制定好的安全策略下进行访问控制，所以一般情况下它是一种静态安全部件，但随防火墙技术的发展，防火墙或通过与 IDS(入侵检测系统)进行联动，或自身集成 IDS 功能，将能够根据实际的情况进行动态的策略调整。

8.1.2　防火墙的功能

防火墙具有如下几个功能：

(1) 访问控制功能。这是防火墙最基本也是最重要的功能，通过禁止或允许特定用户访问特定的资源，保护网络的内部资源和数据。需要禁止非授权的访问，防火墙需要识别哪个用户可以访问何种资源。

(2) 内容控制功能。根据数据内容进行控制，比如防火墙可以从电子邮件中过滤掉垃圾邮件，可以过滤掉内部用户访问外部服务的图片信息，也可以限制外部访问，使它们只能访问本地 Web 服务器中的一部分信息。简单的数据包过滤路由器不能实现这样的功能，但是代理服务器和先进的数据包过滤技术可以做到。

(3) 全面的日志功能。防火墙的日志功能很重要。防火墙需要完整地记录网络访问情况，包括内外网进出的访问，需要记录访问是什么时候进行了什么操作，以检查网络访问情况。就如银行的录像监视系统，记录下整体的营业情况，一旦有什么事发生，就可以看录像，查明事实。防火墙的日志系统也有类似的作用，一旦网络发生了入侵或者遭到破坏，就可以对日志进行审计和查询。日志需要有全面的记录和方便的查询。

(4) 集中管理功能。防火墙是一个安全设备，针对不同的网络情况和安全需要，需要制定不同的安全策略，然后在防火墙上实施，使用中还需要根据情况改变安全策略，而且在一个安全体系中，防火墙可能不止一台，所以防火墙应该是易于集中管理的，这样管理员就可以很方便地实施安全策略。

(5) 自身的安全和可用性。防火墙要保证自身的安全，不被非法侵入，保证正常的工

作。如果防火墙被侵入，防火墙的安全策略被修改，这样内部网络就变得不安全。防火墙也要保证可用性；否则网络就会中断，网络连接就失去意义。

另外防火墙还有如下附加的功能：

(1) 流量控制，针对不同的用户限制不同的流量，可以合理使用带宽资源。

(2) NAT(Network Address Translation，网络地址转换)，是通过修改数据包的源地址(端口)或者目的地址(端口)，来达到节省 IP 地址资源，隐藏内部 IP 地址的功能的一种技术。

(3) VPN(Virtual Private Network，虚拟专用网)，指利用数据封装和加密技术，使本来只能在私有网络上传送的数据能够通过公共网络(Internet)进行传输，使系统费用大大降低。

8.1.3　边界保护机制

对防火墙而言，网络可以分为可信网络和不可信网络。可信网络和不可信网络是相对的，一般来讲内部网络是可信网络，Internet 是不可信网络；但是在内部网络中，比如财务部网络需要特殊保护，在这里财务部网络是可信网络，其他的内部网络就变成了不可信网络。对于服务器来说，比如 Web 服务器、数据库服务器，内部网络和外部网络则都是不可信网络。

防火墙的安放位置是可信网络和不可信网络的边界，它所保护的对象是网络中有明确闭合边界的网段。防火墙是可信网络通向不可信网络的唯一出口，在被保护网络周边形成被保护网络与外部网络的隔离，防范来自被保护网络外部的对被保护网络安全的威胁，所以它是一种边界保护，它对可信网络内部之间的访问无法控制，仅对穿过边界的访问进行控制。

8.1.4　潜在的攻击和可能的对象

防火墙放在可信网络的边界，直接面对的是不可信网络可能的攻击，面临 Internet 中的恶意访问者的攻击。由于大多数主机操作系统和服务存在缺陷、薄弱点和安全漏洞，系统的配置文件不当和口令选择失误都会被恶意破坏者所利用，安全配置错误和失误越来越普遍。恶意破坏者主要有以下几种可能的攻击：

(1) 入侵内部网络。包括没有授权地访问内部网络，盗取信息。比如进行地址欺骗，不可信网络的用户伪装成可信网络的地址，从而绕过系统的认证实现进入被攻击系统；或者通过在内部网络中安装木马程序，实现对内部机器的控制。

(2) 针对防火墙的攻击，使其失去功能。包括各种协议漏洞攻击和碎片攻击，控制防火墙，使防火墙死机或者失去本身应有功能。

(3) 拒绝服务攻击。此种攻击现在非常普遍，对网络的危害非常大，是防火墙较难阻挡的攻击之一。它主要有以下几种方式。

① Syn Flood：该攻击以多个随机的源主机地址向目的主机发送 SYN 包，而在收到目的主机的 SYN ACK 后并不回应，这样，目的主机就为这些源主机建立了大量的连接队列，而且由于没有收到 ACK 一直维护着这些队列，造成了资源的大量消耗而不能向正常

请求提供服务。

② Smurf：该攻击向一个子网的广播地址发一个带有特定请求(如 ICMP 回应请求)的包，并且将源地址伪装成想要攻击的主机地址。子网上所有主机都回应广播包请求而向被攻击主机发包，使该主机受到攻击。

③ Land-based：攻击者将一个数据包的源地址和目的地址都设置为目标主机的地址，然后将该数据包通过 IP 欺骗的方式发送给被攻击主机，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而很大程度地降低了系统性能。

④ Ping of Death：根据 TCP/IP 的规范，一个 IP 包的长度最大为 65 536B，但发送较大的 IP 包时将进行分片，这些 IP 分片到达目的主机时又重新组合起来。在 Ping of Death 攻击时，各分片组合后的总长度将超过 65 536B，在这种情况下会造成某些操作系统的宕机。

⑤ Teardrop：较大的 IP 数据包在网络传递时，数据包可以分成更小的片段。攻击者可以通过发送两段(或者更多)数据包来实现 Teardrop 攻击。第一个包的偏移量为 0，长度为 N，第二个包的偏移量小于 N。为了合并这些数据段，TCP/IP 堆栈会分配超乎寻常的巨大资源，从而造成系统资源的缺乏甚至系统崩溃。

⑥ Ping Sweep：使用 ICMP Echo 轮询多个主机，阻塞网络。

⑦ Ping Flood：该攻击在短时间内向目的主机发送大量 ping 包，造成网络堵塞或主机资源耗尽。

现在的攻击方式在不断地增加，但是主要的攻击方式可以分为以下几种：

(1) 强度攻击(即洪水攻击)。发送大量的无用数据包来堵塞网络带宽，使目标机器无法对正常的请求发生反应。

(2) 协议漏洞攻击。主要是针对系统的协议漏洞进行的攻击。

(3) 应用漏洞攻击。主要是针对系统的应用漏洞进行的攻击，比如针对 IIS 的 Unicode 漏洞的远程控制的攻击，针对 FTP 的漏洞的攻击等。

从原理上来讲，防火墙可以对以上各种攻击进行有效的检测和阻挡，不让这些攻击渗透到内部网络中。

8.1.5　互操作性要求

防火墙是一种安全设备，同时也是一种网络设备，它安放在网络系统中，需要和其他网络设备配合，以适应各种网络环境，这样才能做到安全性和可用性的统一。

防火墙需要适应各种网络环境，这样就要求防火墙除了在安全防护的功能之外，还需要具有各种网络设备的功能，比如路由功能，支持各种路由协议，这样才能和其他的路由器协同工作；VLAN 的支持，这样才能支持划分了 VLAN 的网络；ADSL 的支持，就能对 ADSL 的接入方式提供安全保护。

如果在已有的网络体系中添加防火墙，将可能影响整个网络的结构。所以防火墙要做到尽量配置灵活，使网络的改造工作尽量简单。一般防火墙是充当路由器的角色，但是如果有些环境改变路由比较困难，防火墙就需要工作在二层，作为一个桥接设备来使用，这样就不需要改变路由，网络的结构就不需要改变，另外防火墙可能还需要路由器和桥接

混用的情况，以适应复杂的网络环境。

8.1.6　防火墙的局限性

安装防火墙并不能做到绝对的安全，它有许多防范不到的地方，具体如下：

（1）防火墙不能防范不经由防火墙的攻击。例如，如果允许从受保护网内部不受限制地向外拨号，一些用户可以形成与 Internet 的直接的连接，从而绕过防火墙，造成一个潜在的后门攻击渠道。

（2）防火墙不能防止感染了病毒的软件或文件的传输。这只能在每台主机上装反病毒软件。这是因为病毒的类型太多，操作系统也有多种，不能期望防火墙去对每一个进出内部网络的文件进行扫描，查出潜在的病毒；否则，防火墙将成为网络中最大的瓶颈。

（3）防火墙不能防止数据驱动式攻击。有些表面看起来无害的数据通过电子邮件发送或者其他方式复制到内部主机上，一旦被执行就形成攻击。一个数据型攻击可能导致主机修改与安全相关的文件，使得入侵者很容易获得对系统的访问权。后面将会看到，在堡垒主机上部署代理服务器是禁止从外部直接产生网络连接的最佳方式，能减少数据驱动型攻击的威胁。

（4）防火墙不能防范恶意的内部人员侵入。内部人员通晓内部网络的结构，如果他从内部入侵内部主机，或进行一些破坏活动，因为该通信没有通过防火墙，所以防火墙无法阻止。

（5）防火墙不能防范不断更新的攻击方式，防火墙制定的安全策略是在已知的攻击模式下制定的，所以对全新的攻击方式缺少阻止功能。防火墙不能自动阻止全新的侵入，所以以为安装了防火墙就可以高枕无忧的思想是很危险的。

8.1.7　防火墙的分类

从实现技术方式来分类，防火墙可分为包过滤防火墙、应用网关防火墙、代理防火墙和状态检测防火墙，后面分别详述。

从形态上来分类，防火墙可以分为软件防火墙和硬件防火墙。软件防火墙提供防火墙应用软件，需要安装在一些公共的操作系统上，比如 MS Windows 或者 UNIX，此类防火墙如 Checkpoint 防火墙。硬件防火墙是将防火墙软件安装在专用的硬件平台和专有操作系统（有些硬件防火墙甚至没有操作系统）之上，以硬件形式出现，有的还使用一些专有的 ASIC 硬件芯片负责数据包的过滤。这种方式可以减少系统的漏洞，性能更好，是比较常用的方式，比如 Cisco 的 PIX 防火墙。

8.1.8　防火墙的访问效率和安全需求

防火墙是网络的开放性和安全的控制性矛盾对立的产物。一方面网络的优势是它的互联互通性，用户希望快捷顺畅地访问网站、收发电子邮件等；另一方面，网络也是不安全的，所以需要使用防火墙对网络进行控制，添加安全规则，让用户通过登录来完成访问授权，可这样会使用户感到烦琐，而且需要检查的安全规则越多，网络性能就会越差。所以防火墙的访问效率和安全需求是一对矛盾，应该努力寻找平衡。防火墙的访问效率一般

是指防火墙的性能，根据 RFC2544 网络设备的性能指标，防火墙主要有以下几个性能指标(具体的指标术语由 RFC1242 定义)。

(1) 吞吐量：指防火墙在不丢失数据包的情况下能达到的最大的转发数据包的速率。这个指标反应了防火墙转发包的能力，对网络的性能影响很大，吞吐量是防火墙性能中的一项非常重要的指标。如果防火墙的吞吐量指标太低就会造成网络瓶颈，影响网络的性能。

(2) 时延：对存储转发设备，如路由器，是指从入口处进入的输入帧的最后一个比特到达，到从出口发出的输出帧的第一个比特输出所用的时间间隔。这个指标能够衡量出防火墙处理数据的快慢。

(3) 丢包率：在特定负载下，指应由网络设备传输，但由资源耗尽而丢弃帧的百分比。在连续负载的情况下，指防火墙设备由于资源不足应转发但却未转发的帧所占的百分比。丢包率是衡量防火墙设备稳定性和可靠性的重要指标。

(4) 背对背：指从空闲状态开始，以达到传输介质最小合法间隔极限的传输速率发送相当数量的固定长度的帧，当出现第一个帧丢失时所发送的帧数。背对背的测试结果能够反映出防火墙设备的缓存能力、对网络突发数据流量的处理能力。

(5) 并发连接数：指穿越防火墙的主机之间或主机与防火墙之间能同时建立的最大连接数，并发连接数的测试主要用来测试被防火墙建立和维持 TCP 连接的性能。同时也能够通过并发连接数的大小体现防火墙对来自客户端 TCP 连接请求的响应能力。

在选择防火墙时，应该结合安全需求和防火墙的性能来进行选择。现在网络速度越来越快，对防火墙的要求也越来越高，一般的防火墙都能做到在满足安全需求的情况下保证性能，但是它们一般达不到线速，只有通过专门的数据包过滤芯片才可以使防火墙真正达到线速。

8.2　防火墙技术

8.2.1　包过滤技术

包过滤(packet filtering)技术是防火墙在网络层中根据数据包中包头信息有选择地实施允许通过或阻断。依据防火墙内事先设定的过滤规则，检查数据流中每个数据包头部，根据数据包的源地址、目的地址、TCP/UDP 源端口号、TCP/UDP 目的端口号及数据包头中的各种标志位等因素来确定是否允许数据包通过，其核心是安全策略即过滤规则的设计。一般来说，不保留前后连接信息，利用包过滤技术很容易实现允许或禁止访问。

例如，基于特定的 Internet 服务的服务器驻留在特定的端口号的事实(如 TCP 端口 23 用于提供 Telnet 服务)，使包过滤器可以通过规定适当的端口号来达到阻止或允许到特定服务连接的目的，也可以通过规定协议号，来达到阻止或允许协议的连接，并可进一步组成一套数据包过滤规则。

包过滤技术在防火墙上的应用非常广泛，因为 CPU 用来处理包过滤的时间相对很

小，而且这种防护措施对用户透明，合法用户在进出网络时，根本感觉不到它的存在，使用起来很方便。但是因为包过滤技术是在 IP/TCP 层实现的，所以包过滤的一个很大的弱点是不能在应用层级别上进行过滤，所以防卫方式比较单一。但是现在已经有一些在 IP 层重组应用层数据的技术，从而可以对应用层数据进行检查，可以辨认一些入侵活动，达到很好的防护效果。

包过滤技术作为防火墙的应用有两类：一是路由设备在完成路由选择和数据转发之外，同时进行包过滤，这是目前较常用的方式；二是在一种称为屏蔽路由器的路由设备上启动包过滤功能。

8.2.2　应用网关技术

应用网关(application gateway)与包过滤防火墙不同，它不使用通用目标机制来允许各种不同种类的通信，而是针对每个应用使用专用目的的处理方法。虽然这样做看起来有些浪费，但却比任何其他方法安全得多，因为不必担心不同过滤规则集之间的交互影响及对外部提供安全服务的主机中的漏洞，而只需仔细检查选择的应用程序。

应用网关技术是建立在网络应用层上的协议过滤，它针对特别的网络应用服务协议即数据过滤协议，并且能够对数据包进行分析并形成相关的报告。应用网关对某些易于登录和控制所有输出输入的通信的环境给予严格的控制，以防有价值的程序和数据被窃取。它的另一个功能是对通过的信息进行记录，如什么样的用户在什么时间连接了什么站点。在实际工作中，应用网关一般由专用工作站系统来完成。

有些应用网关还存储 Internet 上那些被频繁使用的页面。当用户请求的页面在应用网关服务器缓存中存在时，服务器将检查所缓存的页面是否是最新的版本(即该页面是否已更新)。如果是最新版本，则直接提交给用户；否则，到真正的服务器上请求最新的页面，然后再转发给用户。

应用层网关的优点是它易于记录并控制所有的进出通信，并对 Internet 的访问做到内容级的过滤，控制灵活而全面，安全性高。应用级网关具有登记、日志、统计和报告功能，有很好的审计功能，还可以具有严格的用户认证功能。

应用层网关的缺点是需要为每种应用写不同的代码，维护比较困难，另外就是速度较慢。

8.2.3　状态检测防火墙

状态检测(stateful inspection)防火墙现在应用非常广泛，状态检测是一种相当于 4.5 层的过滤技术，它不限于包过滤防火墙的 3/4 层的过滤，又不需要应用层网关防火墙的 5 层过滤，既提供了比包过滤防火墙更高的安全性和更灵活的处理，也避免了应用层网关防火墙带来的速度降低的问题。

要实现状态检测防火墙，最重要的是实现连接的跟踪功能。对于单一连接的协议来说相对比较简单，只需要数据包头的信息就可以进行跟踪；但对于一些复杂协议，除了使用一个公开端口的连接进行通信外，在通信过程中还会动态建立子连接进行数据传输，而子连接的端口信息是在主连接中通过协商得到的随机值，因此对于此类协议，用包过滤防

火墙就只能打开所有端口才能允许通信，但这会带来很大的安全隐患。而对于状态检测防火墙，则能够进一步分析主连接中的内容信息，识别出所协商的子连接的端口而在防火墙上将其动态打开，连接结束时自动关闭，充分保证系统的安全。如使用 FTP 协议进行数据传送时是通过另一个子连接进行的，状态检测防火墙能够通过跟踪主连接中的信息得到子连接所用的端口，自动确定允许此连接的数据通过而不必另加规则。使用多个连接的协议，除了 FTP 协议外，还有一些数据库通信使用的协议、多媒体通信使用的协议等，状态检测防火墙为能跟踪这些协议，就必须单独为各协议实现连接跟踪模块，而且一般要求这些协议在协商子连接端口时是明文协商，不能进行加密。

8.2.4　电路级网关

电路级网关也被称为线路级网关，它工作在会话层。它在两个主机首次建立 TCP 连接时创立一个电子屏障。它作为服务器接收外来请求，转发请求；与被保护的主机连接时则担当客户机角色，起代理服务的作用。它监视两主机建立连接时的握手信息，如 SYN、ACK 等标志和序列号等是否合乎逻辑，判定该会话请求是否合法。一旦会话连接有效后网关仅复制、传递数据，而不进行过滤。电路网关中特殊的客户程序只在初次连接时进行安全协商控制，其后就透明了。只有懂得如何与该电路网关通信的客户机才能到达防火墙另一边的服务器。在不同方向上拒绝发送上传和获取命令，就可限制 FTP 服务的使用。如不允许上传命令输入，外部用户就不能将文件上传到 FTP 服务器破坏其内容；如不允许上传命令输出，则不可能将信息存储在网点外部的 FTP 服务器上。

电路级网关的防火墙的安全性比较高，但它仍不能检查应用层的数据包以消除应用层攻击的威胁。

8.2.5　代理服务器技术

代理服务器（proxy server）作用在应用层，它用来提供应用层服务的控制，在内部网络向外部网络申请服务时起到中间转接作用。内部网络只接受代理提出的服务请求，拒绝外部网络其他结点的直接请求。

具体地说，代理服务器是运行在防火墙主机上的专门的应用程序或者服务器程序；防火墙主机可以是具有一个内部网络接口和一个外部网络接口的双重宿主主机，也可以是一些可以访问 Internet 并被内部主机访问的堡垒主机。这些程序接受用户对 Internet 服务的请求（诸如 FTP、Telnet），并按照一定的安全策略将它们转发到实际的服务中。代理提供代替连接并且充当服务的网关。

包过滤技术和应用网关通过特定的逻辑判断来决定是否允许特定的数据通过。其优点是速度快、实现方便。缺点是审计功能差，过滤规则的设计存在矛盾关系，即如果过滤规则简单，则安全性差；如果过滤规则复杂，则管理困难。一旦判断条件满足，防火墙内部网络的结构和运行状态便“暴露”在外来用户面前。代理技术则能进行安全控制和加速访问，有效地实现防火墙内外计算机系统的隔离，安全性好，以及实施较强的数据流监控、过滤、记录和报告等功能。其缺点是对于每一种应用服务都必须为其设计一个代理软件模块来进行安全控制，而每一种网络应用服务的安全问题各不相同，分析困难，因此实现也

困难。

在实际应用当中，构筑防火墙的“真正的解决方案”很少采用单一的技术，通常是多种解决不同问题的技术的有机组合。用户需要解决的问题依赖于他想要向其客户提供什么样的服务以及愿意接受什么等级的风险，采用何种技术来解决那些问题依赖于用户的时间、金钱、专长等因素。

一些协议（如 Telnet、SMTP）能更有效地处理数据包过滤，而另一些（如 FTP、Gopher、WWW）能更有效地处理代理。大多数防火墙将数据包过滤和代理服务器结合起来使用。

8.3　防火墙体系结构

8.3.1　双重宿主主机体系结构

双重宿主主机体系结构围绕双重宿主主机构筑。双重宿主主机至少有两个网络接口。这样的主机可以充当外部网络和内部网络之间的路由器，所以它能够使内部网络和外部网络的数据包直接路由通过。然而双重宿主主机的防火墙体系结构不允许这样直接地通过。因此 IP 数据包并不是从一个网络（如外部网络）直接发送到另一个网络（如内部网络）。外部网络能与双重宿主主机通信，内部网络也能与双重宿主主机通信，但是外部网络与内部网络不能直接通信，它们之间的通信必须经过双重宿主主机的过滤和控制，它安装了防火墙的软件，一般在双重宿主主机上安装代理服务器软件，可以为不同的服务提供转发，并同时根据策略进行过滤和控制。

双重宿主主机体系结构是比较简单的，它连接内部网络和外部网络。它相当于内部网络和外部网络的跳板，能够提供级别比较高的控制，可以完全禁止外部网络对内部网络的访问。这种结构可以允许用户登录到双重宿主主机，进而访问外部网络，但是这种控制方式是不安全的，因为外部网络用户也有可能登录并访问内部网络，而且这种访问外部网络的方式对内部网络用户来讲也是很麻烦的。

这种情况下，双重宿主主机直接暴露在外部网络中，充当了堡垒主机的角色，这种体系的弱点是，一旦堡垒主机被攻破，使其成为一个路由器，那么外部网络就可以直接访问内部网络。具体结构如图 8-2 所示。

8.3.2　被屏蔽主机体系结构

双重宿主主机体系结构防火墙没有使用路由器。而被屏蔽主机体系结构防火墙则使用一个路由器把内部网络和外部网络隔离开，如图 8-3 所示。在这种体系结构中，主要的安全由数据包过滤提供（例如，数据包过滤用于防止人们绕过代理服务器直接相连）。

这种体系结构中包括堡垒主机。堡垒主机是 Internet 上的主机能连接到的唯一的内部网络上的系统。任何外部的系统要访问内部的系统或服务都必须先连接到这台主机。因此堡垒主机要保持更高等级的主机安全。在屏蔽路由器上设置数据包过滤策略，让所

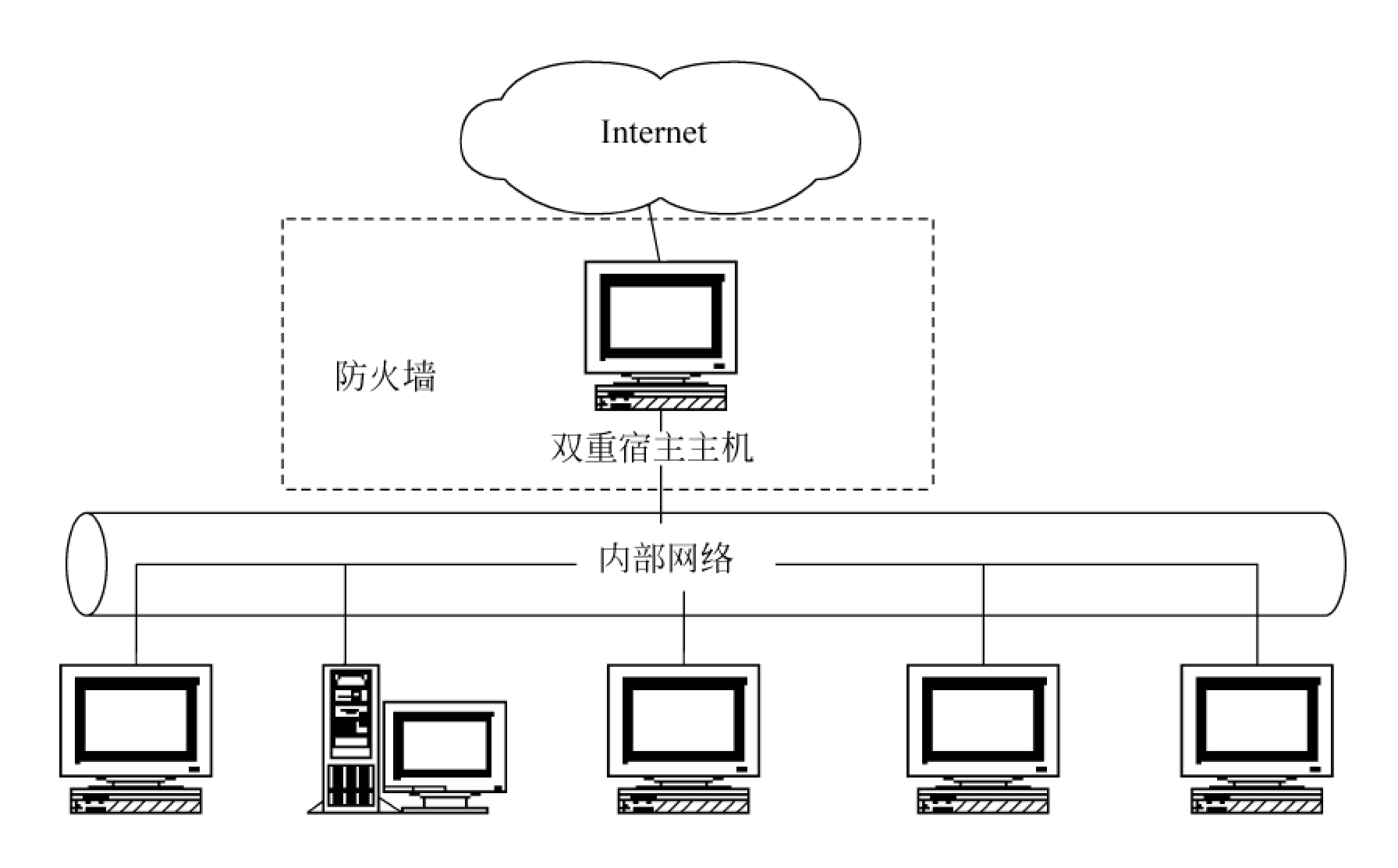


图 8-2　双重宿主主机体系结构

有的外部连接只能到达内部堡垒主机，比如收发电子邮件。

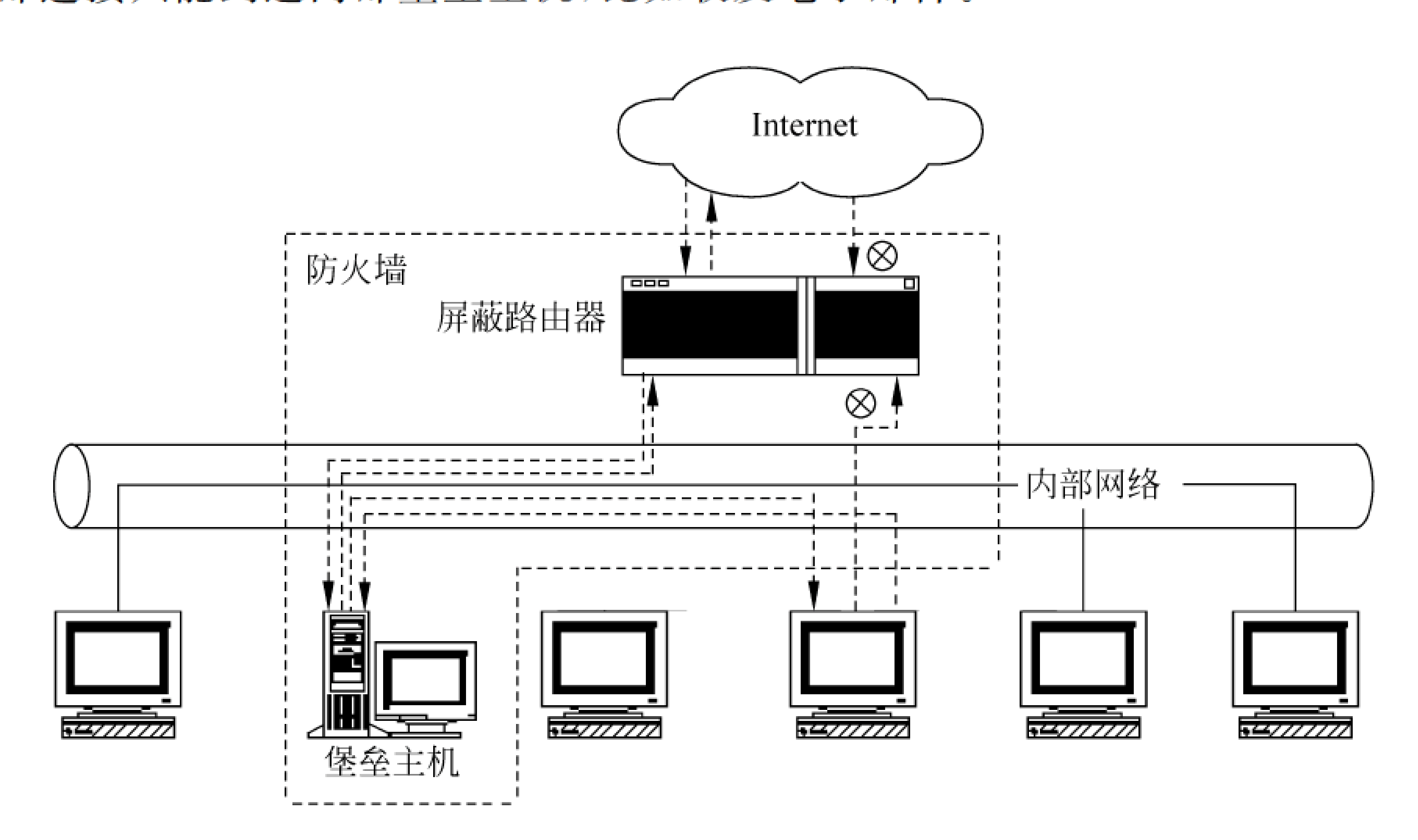


图 8-3　被屏蔽主机体系结构

数据包过滤允许堡垒主机开放到外部网络的可允许的连接。在屏蔽的路由器中数据包过滤策略可以按下列方案之一设置：

（1）允许其他的内部主机为了某些服务开放到 Internet 上的主机连接（允许那些经由数据包过滤的服务）。

（2）不允许来自内部主机的所有连接（强迫那些主机经由堡垒主机使用代理服务）。

（3）对于内部用户对外部网络的访问，可以强制其经过堡垒主机，也可以让其直接经过屏蔽路由器出去，针对不同的应用采用不同的安全策略。

这种体系允许外部连接到内部堡垒主机，所以看上去比双重堡垒主机更不安全，但是路由器一般比主机有更高的安全性，所以这种结构比双重堡垒主机更具有可用性和安全

性。但是这种结构相对比较复杂。

8.3.3　被屏蔽子网体系结构

被屏蔽子网体系结构将额外的安全层添加到被屏蔽主机体系结构，即通过添加周边网络更进一步地把内部网络和外部网络(通常是 Internet)隔离开。

周边网络是一个被隔离的独立子网，充当了内部网络和外部网络的缓冲区，在内部网络与外部网络之间形成了一个“隔离带”。这就构成一个所谓的“非军事区”(DeMilitarized Zone，DMZ)，DMZ 是周边网络，是防火墙的重要概念，在实际应用中经常用到。

被屏蔽子网体系结构的最简单的形式是两个屏蔽路由器，每一个都连接到周边网络。一个位于周边网络与内部网络之间，另一个位于周边网络与外部网络(通常为 Internet)之间，如图 8-4 所示。有的屏蔽子网中还设有一堡垒主机作为唯一可访问点，支持终端交互或作为应用网关代理。为了侵入用这种体系结构构筑的内部网络，非法入侵者必须通过这两个路由器。即使非法入侵者侵入堡垒主机，它仍将必须通过内部路由器。

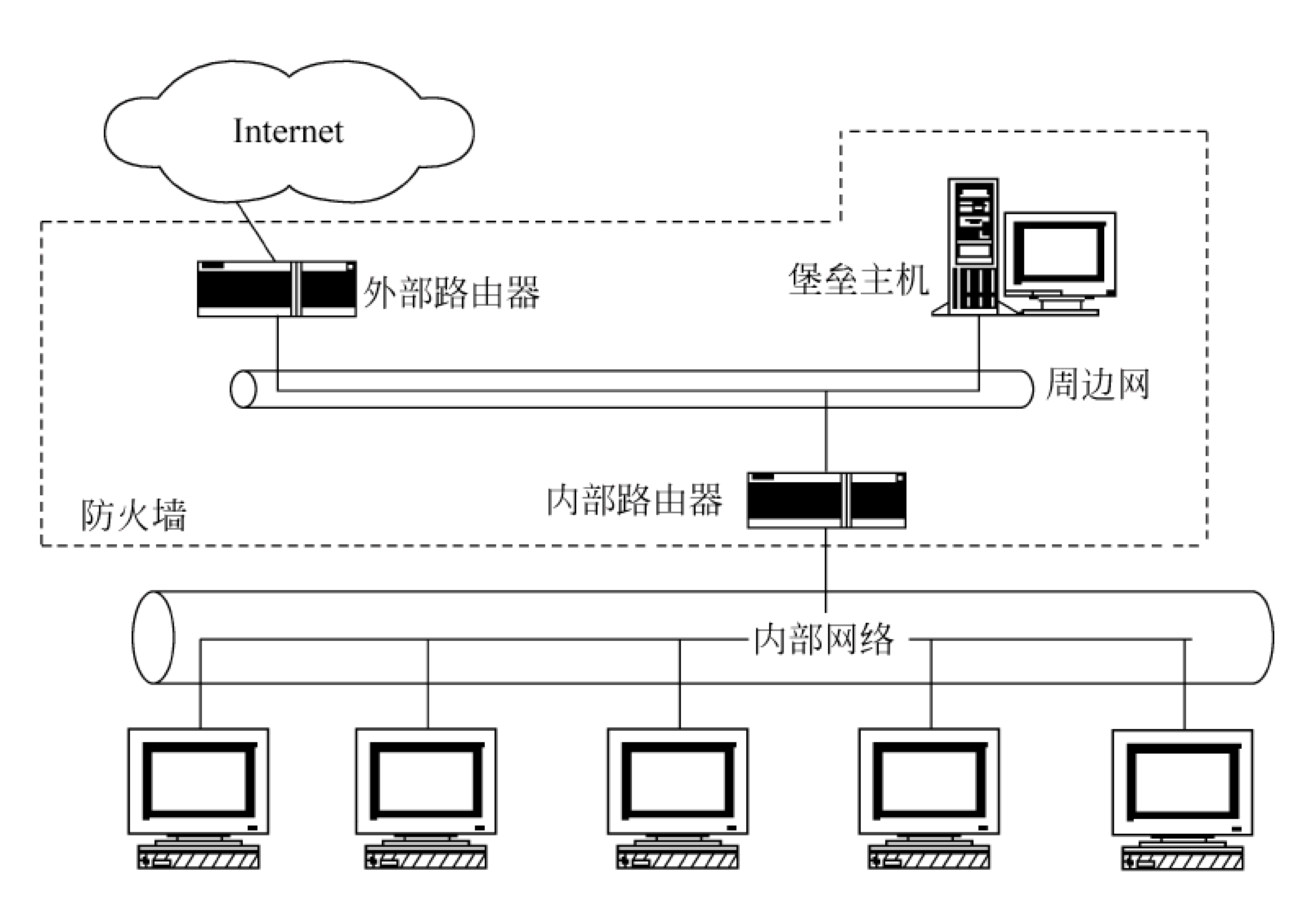


图 8-4　被屏蔽子网体系结构

如果攻击者试图完全破坏防火墙，它必须重新配置连接 3 个网络的路由器，既不切断连接又不把自己锁在外面，同时又不使自己被发现，这样做是可能的。但若禁止网络访问路由器或只允许内部网络中的某些主机访问它，则攻击会变得很困难。在这种情况下，攻击者要先侵入堡垒主机，然后进入内部网络主机，再返回来破坏屏蔽路由器，而且在整个过程中不能引发报警。

这种体系结构具有很高的安全性，所以被广泛采用。

被屏蔽子网体系机构具有以下优点：

(1) 入侵者必须突破 3 个不同的设备(而且外部网络无法探测到)才能非法入侵内部网络、外部路由器、堡垒主机，还有内部路由器。

(2) 由于外部路由器只能向 Internet 通告 DMZ 网络的存在，Internet 上的系统没有路由器与内部网络相通。这样网络管理员就可以保证内部网络是“不可见”的，并且只有在 DMZ 网络上选定的服务才对 Internet 开放。

(3) 由于内部路由器只向内部网络通告 DMZ 网络的存在，内部网络上的系统不能直接通往 Internet，这样就保证了内部网络上的用户必须通过驻留在堡垒主机上的代理服务才能访问 Internet。

(4) 包过滤路由器直接将数据引向 DMZ 网络上所指定的系统，消除了堡垒主机双重宿主的必要。

(5) 内部路由器在作为内部网络和 Internet 之间最后的防火墙系统时，能够支持比双重宿主堡垒主机更大的数据包吞吐量。

(6) 由于 DMZ 网络是一个与内部网络不同的网络，NAT(网络地址变换)可以安装在堡垒主机上，从而避免在内部网络上重新编址或重新划分子网。

这个结构的缺点是实施和管理比较复杂。

8.4　堡垒主机

在防火墙体系结构中，经常提到堡垒主机，堡垒主机得名于古代战争中用于防守的坚固的堡垒，它位于内部网络的最外层，像堡垒一样对内部网络进行保护。在防火墙体系中，堡垒主机要高度暴露，是在 Internet 上公开的，是网络上最容易遭受非法入侵的设备。所以防火墙设计者和管理人员需要致力于堡垒主机的安全，而且在运行期间对堡垒主机的安全给予特别的注意。

构建堡垒主机的要点如下：

(1) 选择合适的操作系统。它需要可靠性好、支持性好、可配置性好。

(2) 堡垒主机的安装位置。堡垒主机应该安装在不传输保密信息的网络上，最好它处于一个独立网络中，比如 DMZ。

(3) 堡垒主机提供的服务。堡垒主机需要提供内部网络访问 Internet 的服务，内部主机可以通过堡垒主机访问 Internet，另外内部网络也需要向 Internet 提供服务。

(4) 保护系统日志。作为一个安全性举足轻重的主机，堡垒主机必须有完善的日志系统，而且必须对系统日志进行保护。

(5) 监测和备份。最简单的方式是把备份存储到与堡垒主机直接相连的磁带机上。

8.5　数据包过滤

8.5.1　数据包过滤的特点

数据包过滤的安全策略基于以下几种方式：

(1) 数据包的源地址。

(2) 数据包的目的地址。

(3) 数据包的 TCP/UDP 源端口。

(4) 数据包的 TCP/UDP 目的端口。

(5) 数据包的标志位。

(6) 用来传送数据包的协议。

一般的包过滤防火墙对数据包数据内容不做任何检查(有些可以),而只检查数据包头信息。数据包过滤在网络中起着重要的作用,可以在单点位置为整个网络提供安全保护。以 WWW 服务为例,如果不想让外部用户访问内部的 WWW 服务,可以通过关闭所有主机上的 WWW 服务做到,但是如果有人新装了一台机器并且启动了 WWW 服务,安全性就会被破坏。而只要在包过滤路由器上加上安全规则,禁止外部对内部 WWW 服务(TCP 80 端口)的访问,则无论是否所有的内部网络主机都启动了 WWW 服务,它们都将得到保护,这样做很容易也很安全。数据包过滤对用户是透明的,不要求内部网络用户进行任何配置。

作为网络边界的数据包过滤路由器可以提供一些特别的保护,比如可以拒绝所有来自于外部,却具有内部源地址的数据包,这就是常用的一种入侵方式——IP 地址欺骗。因为数据包过滤路由器处于网络边界,很容易判断数据包是来自于外部还是内部,这样就很容易阻挡 IP 地址欺骗入侵。

但是数据包过滤也是有局限的,其局限性表现如下:

(1) 不能进行内容级控制,如针对用户身份进行限制,不能做到对于一个 Telnet 服务器,禁止 user1 登录,而允许 user2 登录;因为用户名是数据包内容部分的信息,过滤系统不能辨认从而无法控制。另如,不能针对于一个 FTP 服务器,允许用户下载某些文件,而禁止用户下载某些文件;因为文件名也属于数据包内容,所以不能辨认。

(2) 数据包的过滤规则制定比较复杂,需要针对不同的 IP 或者服务制定很多的安全规则,而且过滤规则会存在冲突或者漏洞,检查起来相对困难。

(3) 有些协议不适合包过滤。

8.5.2 数据包过滤的应用

现在 Internet 广泛采用 TCP/IP 协议,TCP/IP 协议簇遵守一个 4 层的参考模型,包括接口层、网络层、传输层和应用层。下面分析数据包过滤在各层协议中的应用。

1. IP 协议

对于数据包过滤,IP 层有几个重要的信息,可以依据这些信息制定相应的安全策略:

(1) IP 源地址,32 位。

(2) IP 目的地址,32 位。

(3) IP 协议类型,辨别 TCP 数据包类型和 ICMP 数据包类型。

(4) IP 选项字段。

可以根据 IP 协议中的 IP 源地址和 IP 目的地址来制定安全规则,数据包过滤面对的

最普遍的 IP 选项字段是源地址路由，源地址路由是由数据包的源地址来指定到达目的地的路由，而不是让路由器根据其路由表来决定向何处发送数据包。这种功能有的时候是有用的，比如路由器的路由表发生了损坏；但是有的时候也会被黑客所利用，企图绕过安全检测，而不走预先设计好的路由路径。这种类型的攻击是为了旁路安全措施并导致数据包循着一个对方不可预料的路径到达目的地，另外它还将成为 IP 地址欺骗攻击的辅助手段，来实现欺骗的 IP 地址能够正常路由，并且能够收到回应。

解决这个问题的办法很简单，只要检查 IP 选项，简单地丢弃所有包含源路由选项的数据包即可。这样做既可保证安全，也不会影响正常的访问。

IP 协议的特点之一就是将一个大的数据包划分成若干个适合大小的、能通过网络传送的 IP 片，称为 IP 分片。IP 分片到达目标机器后，再重新组装成完整的 IP 数据包。对于数据包过滤，只有在第一个分片中才包含来自于高层协议的报头信息，数据包过滤可以检查这个段，根据报头来决定是否允许整个数据包通过。如果禁止该数据包，数据包过滤只是丢弃了 IP 分片的第一个分片，其他的分片还是能够通过。但是不管有多少个分片通过，目标机器都不能将这些段装配成原来的数据包，因为第一个分片已经没有了。但是这样做也是有危险的，因为目标机器会将收到的分片在内存中保留一段时间，等待首段的到来，这使黑客有可能利用分片数据包进行拒绝服务攻击，使目标计算机不能工作。当目标主机不能组装数据包时，它会发送一个 ICMP 数据包组装超时的消息返回，这样黑客就知道该主机是存在的，以及为什么连接不成功。除非进行设置过滤掉这些 ICMP 信息。当允许外部请求进入，禁止应答的时候，应答的首片被禁止，但是其他的分片将流出，黑客就可以得到它们，并进行分析得到它们想得到的东西。

极小数据段式攻击（Tiny Fragment Attacks）的特点是入侵者使用了 IP 分片的特性，创建极小的分片并强行将 TCP 头信息分成多个数据包段。这种攻击是为了绕过用户定义的过滤规则。黑客寄希望于过滤器，路由器只检查第一个分片而允许其余的分片通过。

2. TCP 协议

针对数据包过滤，TCP 层有几个重要的信息：

(1) TCP 源端口。

(2) TCP 目标端口。

(3) TCP 标志字段。

可以根据 TCP 协议中的源端口和目的端口来制定安全规则，因为 TCP 的源端口通常是随机的，所以通常不使用源端口进行控制。通过检查 TCP 标志字段，可以辨认这个 TCP 数据包是 SYN 包，还是非 SYN 包。检查单独的 SYN 标志，就可以知道它是 TCP 连接中 3 次握手中的第一个请求，如果要禁止该连接，只要禁止这个包就可以了。

3. UDP 协议

针对数据包过滤，UDP 协议有几个重要的信息：

(1) UDP 源端口。

(2) UDP 目标端口。

可以根据 UDP 协议中的源端口和目的端口来制定安全规则。因为 UDP 的源端口

通常是随机的，所以通常不使用源端口进行控制。

4. ICMP 协议

ICMP 即 Internet 控制与报文协议，由 RFC792 定义，这个协议主要用来进行错误信息和控制信息的传递，例如，著名的 Ping 工具是利用 ICMP 协议中的 ECHO request 报文进行的(请求报文 ICMP ECHO 类型 8 代码 0，应答报文 ICMP ECHOREPLY 类型 0 代码 0)。

ICMP 协议有一个特点，它是无连接的，也就是说只要发送端完成 ICMP 报文的封装并传递给路由器，这个报文将会像邮包一样自己去寻找目的地址。这个特点使得 ICMP 协议非常灵活快捷，但是同时也带来一个缺陷就是易伪造(邮包上的寄信人地址是可以随便写的)。任何人都可以伪造一个 ICMP 报文并发送出去，伪造者可以直接改写报文的 ICMP 首部和 IP 首部，这样的报文携带的源地址是伪造的，在目的端根本无法追查，根据这个原理，出现了不少基于 ICMP 的攻击软件，有通过网络架构缺陷制造 ICMP 风暴的，有使用非常大的报文堵塞网络的，有利用 ICMP 碎片攻击消耗服务器 CPU 的，甚至有将 ICMP 协议用于通信，制作出的不需要任何 TCP/UDP 端口的木马。

包过滤器一般禁止从外部网络来的到内部网络和包过滤器本身的 ICMP 包，这样就可以避免危险。

8.5.3　过滤规则制定的策略

1. 按地址过滤

按地址过滤是最简单的过滤方式，它只限制数据包的源地址和目的地址，而不必考虑协议。如果限制源地址，就会面临风险，因为源地址是可以伪造的，前面已经分析过，如果外部用户伪装成内部用户的 IP 地址，数据包过滤路由器可以很好地防护，但是如果只允许特定的外部主机访问内部网络，此时如果另一个主机伪装成特定的外部主机，过滤器就无能为力了。

在源地址伪装侵入中，黑客可以伪装成用户信任的外部主机，但是内部主机的回应却不会到达黑客那里，此时黑客也能完成入侵。但是它们可以通过其他方法更方便地实现入侵，比如当信任主机出现故障时，如通过拒绝服务攻击使信任主机崩溃而失去反应，黑客就可以取代信任主机进行入侵，具体步骤如下：

① 假定有一个黑客，A 和 B 是合法用户，B 位于防火墙内部，并且防火墙允许外部网络中的 A 主机的 IP 地址访问 B 主机。为达到假冒目的，黑客通过一个打开端口连接到 A 的计算机，然后查看 A 的计算机初始序列号(ISN)并分析它们是如何变化的，得到序列号的变化规律，当然也可能完全靠猜测得到序列号，因为如果 TCP 实现时未使用好的序列号初始化算法的话，固定的、有规律的序列号变化是可以进行猜测的。

② 利用 ISN 信息，针对 A 执行一次 DOS 攻击，使主机 A 崩溃，失去反应能力。然后黑客用 A 的地址给 B 发一个消息。B 照例用 3 次握手的第二部分对 A 做出答复。黑客模仿 A 用应答(ACK)和前面发现的已增加的 ISN 发送 3 次握手的最后一部分。

③ 成功完成以上步骤后，黑客就与 B 的计算机建立了一个连接并可以开始发送命令

了。现在黑客可以尝试重新配置 B 的计算机，以便让 B 所有的回复都直接发送给自己而不是给 A 主机，如图 8-5 所示。

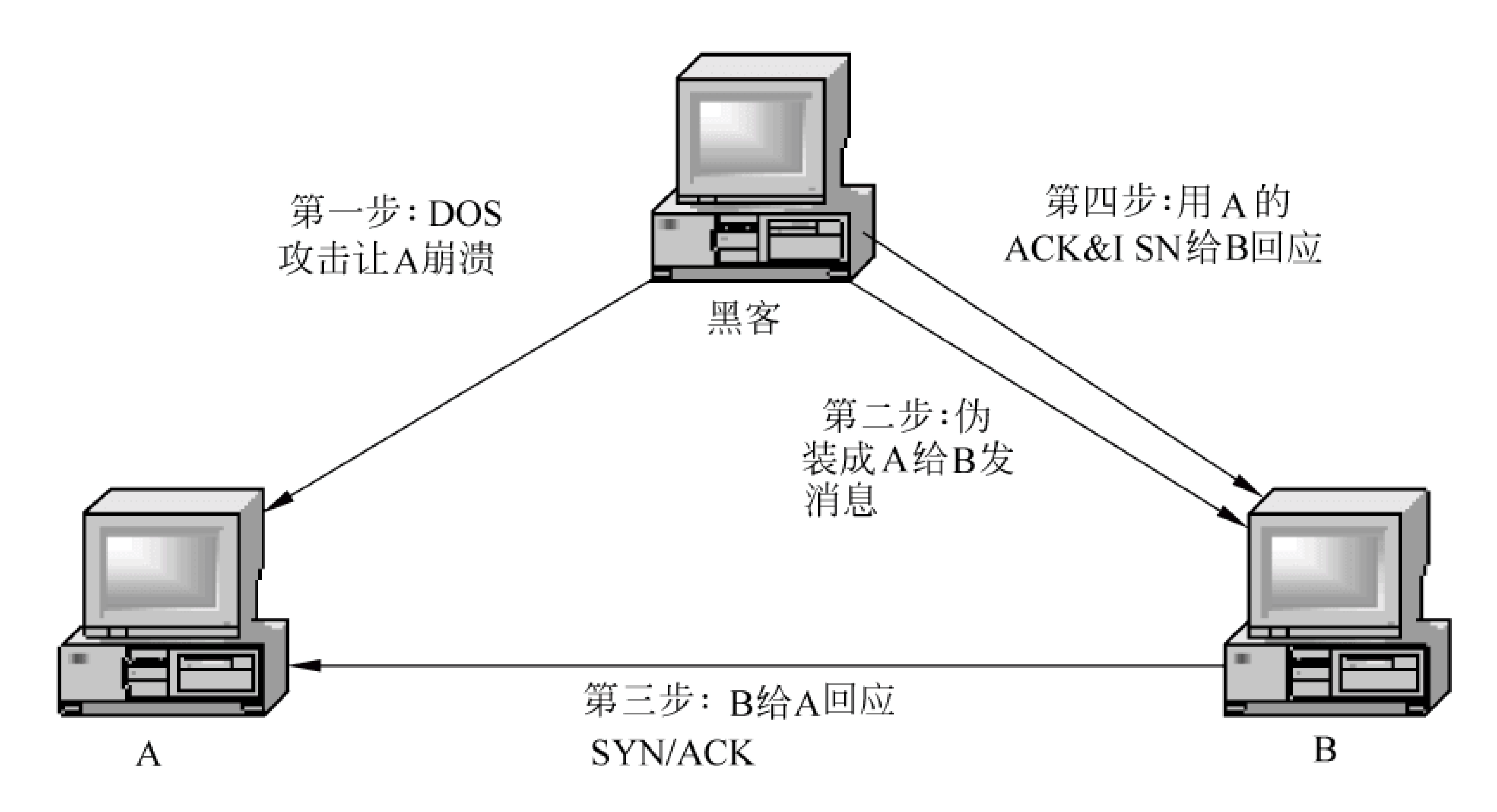


图 8-5　IP 欺骗攻击

所有类型的假冒攻击都是一种严重的威胁，可以用下列方法来对付：

（1）防火墙不制定针对外部网络 IP 地址的信任关系。

（2）确保 ISN 真正是随机的，而且很难预测。

（3）关闭 IP 源路由。

2 按服务过滤

按服务过滤，就是根据相应的 TCP/UDP 端口进行过滤，比如禁止外部网络对内部网络的 Telnet 的访问，就需要检查数据包的目的端口和 TCP 标志位，如果是端口 23，并且是 SYN 包，则拒绝这个包。在实际应用中，一般使用的是目的端口过滤，对于源端口过滤也是有风险的，由上面的分析可知，源端口也是可以伪装的。并且也需要保证内部的服务确实是在相应的端口上。

但是无法保证外部的服务确实是在常规的端口上，如果防火墙的限制完全基于外部主机的端口号，例如，配置允许内部主机到外部服务器的邮件发送服务，当 TCP 端口 25 确是一个常规邮件端口时，这个配置就没有危险，但是防火墙没有办法控制一个外部主机上的端口号。黑客可能会用其他程序从这个主机上的端口 25 发向内部主机，建立连接，进行非授权的访问。

解决这个问题的办法是根据协议的双向性，禁止 25 端口对内部主机的访问，也就是对外部的端口取消信任。

在内部到外部的 TCP 和 UDP 连接中，内部主机采用的源端口一般是大于 1024 的随机端口，这样给过滤规则增加了困难。需要允许返回的到内部主机的大于 1024 端口的数据包都要允许。对于 TCP 连接来说，可以通过 TCP 协议的 flag 位来辨认从外部到内部的连接请求，从而可以阻止对高于 1024 端口的非法连接。而 UDP 是无连接的协议，没有标准可以区分，只能通过端口号。但是端口号是可以伪造的，如果返回的数据包不是到主机随机产生的端口，而是到另一个端口，可能就是一次破坏服务器的尝试。所以允许

UDP 协议的对外访问是有风险的。但是有些 UDP 协议却没有这样的问题,因为它们的请求端口和目的端口都是固定的,这样防火墙只需简单地允许相应的端口的进出就可以保证安全了。

3. 对数据包做日志记录

数据包过滤路由器应该详细记录所有被过滤掉的数据包,这样就可以了解过滤规则阻止了哪些访问,也可以了解究竟哪些人试图违反规则。当然,记录所有通过的数据包也是一个保险的措施,虽然这样需要很多的存储空间,但是为了解决问题,这样做也是值得的。

8.5.4　数据包过滤规则

在配置数据包过滤规则之前,需要明确要允许或者拒绝什么服务,并且需要把策略转换成为针对数据包的过滤规则。

网络协议一般都是双向的,如果发送了一个请求或者一条命令,另一边的主机就会发出某种响应,所以在规划数据包过滤规则时,一定要注意数据包是双向的。例如想允许某个主机访问 Telnet 服务器,但是设置规则时只允许 Telnet 的命令的方向能通过,没有允许返回的数据包通过,这样还是不能访问的。

当想禁止某个用户访问 Telnet 服务器时,设置单向规则也是没有用的,如果设置规则允许 Telnet 的命令的方向可以通过,而不允许返回的数据包通过,入侵也是有可能得逞的。因为一个娴熟的黑客是可以预见 Telnet 服务所具有的返回数据包的,就好像在一个没有显示器的主机上仍然可以完成复制动作一样,它仍然可以间接地获取数据,比如将数据发送到其他主机或者邮件中。

在数据包过滤规则中有两种基本的安全策略:默认接受和默认拒绝。默认接受是指除非明确地指定禁止某个数据包;否则数据包是可以通过的。而默认拒绝则相反,它是除非明确地指定允许某个数据包通过;否则数据包是不可以通过的。从安全的角度讲,默认拒绝应该是更安全的。

建立数据包过滤规则需按如下步骤去做:

① 建立安全策略(写出所允许的和禁止的任务)。

② 将安全策略转化为数据包分组字段的逻辑表达式。

③ 用防火墙提供的过滤规则句法重写逻辑表达式并设置。

首先要针对网络的具体情况制定需要保护什么、需要对外提供什么样的服务的安全策略。主要考虑两个方面,一是内部网络需要访问外部网络的什么服务,如 WWW、FTP、电子邮件等;二是需要给外部网络提供什么服务,因为外部网络是不安全的,因此要特别小心,这个口子开得越小越好。

通过制定数据包过滤规则来控制哪些数据包可以进入或者流出内部网络。在制定了数据包规则后,对于每一个数据包,路由器会从第一条规则进行检查,直到找到一个可以匹配它的规则,然后根据规则来决定是接受还是拒绝整个数据包;如果规则表中没有匹配的规则,则根据设置的安全策略进行处理,如默认拒绝,则这个数据包将被拒绝。

8.6 状态检测的数据包过滤

状态检测防火墙对每个合法网络连接保存的信息包括源地址、目的地址、协议类型、协议相关信息(如 TCP/UDP 协议的端口、ICMP 协议的 ID 号)、连接状态(如 TCP 连接状态)和超时时间等,防火墙把这些信息叫做状态。通过状态检测,可实现比简单包过滤防火墙具有更大的安全性。

当防火墙接收到初始化 TCP 连接的 SYN 包时,要对这个带有 SYN 的数据包进行安全规则检查。将该数据包在安全规则里依次比较,如果在检查了所有的规则后,该数据包都没有被接受,那么拒绝该次连接。如果该数据包被接受,那么本次会话的连接信息被添加到状态监测表里。该表位于防火墙的状态检测模块中。对于随后的数据包,就将包信息和该状态监测表中所记录的连接内容进行比较,如果会话是在状态表内,而且该数据包状态正确,该数据包被接受;如果不是会话的一部分,该数据包被丢弃。这种方式提高了系统的性能,因为不是每一个数据包都要和安全规则比较。只有在新的请求连接的数据包到来时才和安全规则比较。所有的数据包与状态检测表的比较都在内核模式下进行,所以执行速度很快。

状态检测防火墙的理论基础是使用客户机/服务器模式进行的连接具有连接状态,最典型的是 TCP 连接,TCP 连接由 11 个状态组成,其状态转换如图 8-6 所示。在 TCP 包头中有 6 个标志位:FIN、SYN、RST、PSH、ACK、URG。最初双方软件未启动时都处于 CLOSED 状态,当服务器启动后,将打开某一 TCP 端口而进入 LISTEN 状态,等待 TCP 客户端的连接,客户端程序启动后要向服务器连接,客户端向服务器发送 SYN 连接请求包,使客户端进入 SYN_SEND 状态,服务器接收到 SYN 包后如果允许客户端连接将发送 SYN_ACK 包,确认连接,服务器端进入 SYN_RCVD 状态,客户端接收到 SYN_ACK 包后发送一个确认 ACK 包,客户端进入 ESTABLISHED 状态,服务端接收到该 ACK 包后也进入 ESTABLISHED 状态,此即 TCP 协议的 3 次握手过程,连接建立后就可以进行 TCP 数据传输了。TCP 的断开过程比较复杂,这里只描述正常断开过程,其他如同时断开、异常断开等可按图 8-6 同理分析。正常断开是连接一方先发送 FIN 包(连接双方都可以先发送 FIN 包),为叙述方便,假设是服务器端发送 FIN 包,此时服务器端进入 FIN_WAIT_1状态,客户端接收到 FIN 包后,将回应一个 ACK 包,客户端进入 CLOSE_WAIT 状态,服务器端接收到此 ACK 包后进入 FIN_WAIT_2 状态,此时 TCP 连接属于半关闭状态,在此状态下服务器将不再向客户端发送数据,但客户端仍然可以向服务器发送数据,如果客户端也不再发送数据,将发送 FIN 包,客户端进入 LASK_ACK 状态,服务器接收到客户端的 FIN 包后发送一个 ACK 包确认,服务器端进入 TIME_WAIT 状态,客户端收到此 ACK 包后进入 CLOSED 状态,客户端就认为 TCP 连接已经结束,而服务器端再经过 2 倍 MSL(Maximum Segment Lifetime)超时后进入 CLOSED 状态,连接断开,在这段过程中各种 TCP 实现可能会略有差异,MSL 时间也可能有差别。

从以上的 TCP 连接建立和断开描述中可以看出,第一,TCP 连接是有状态的,连接

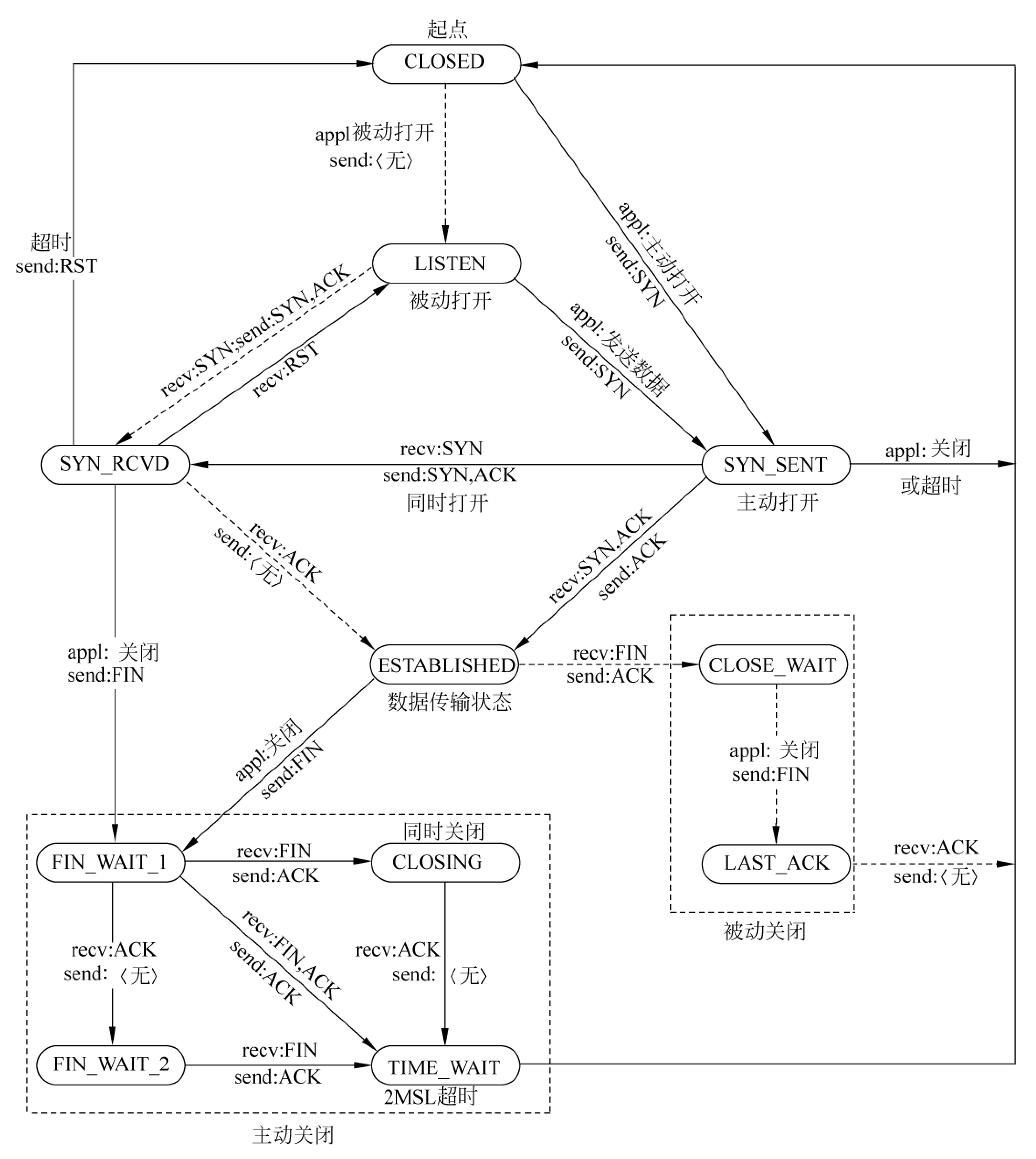


图 8-6　TCP 状态转换图

进入不同的阶段有不同的状态；第二，TCP 连接状态的转换是有一定顺序的，不是任意改变的；第三，TCP 连接过程中客户端和服务端的可能的状态是有区别的，如客户端不可能进入 LISTEN 状态，服务端也不可能进入 SYN_SEND 状态；第四，对于 TCP 包中的标志，有些标志是不能同时存在的，如 SYN 标志不可能和 FIN、RST、PSH 标志同时存在，如同时存在必是伪造包，非正常包。根据以上原则，防火墙作为连接双方的“旁观者”，就

可以判断出连接双方目前处于何种状态。一旦发现所发送包和状态不符,就可认为是状态异常的包进行拒绝,而不必再对 IP 地址或 TCP 端口进行检查;对于一些端口扫描工具进行 TCP 端口扫描时不再发送 SYN 包,而是相对异常的一些 TCP 标志包,如 FIN、RST、SYN_FIN 等;而防火墙对于一个新 TCP 连接的判断是从 SYN 包开始的,一旦发现这些包不属于任何已经建立的连接,就可将其作为状态异常包而丢弃。

对于其他非连接协议,如 UDP、ICMP 等协议,防火墙同样也会建立连接来进行跟踪。对于 UDP 协议,一方发出 UDP 包后,如 DNS 请求,防火墙会将从目的地址和端口返回的、到达源地址源端口的包作为状态相关的包而允许通过;对于 ICMP 协议,如 ping (echo)包,其状态相关包就是来自目的地址的 echo reply 包,而没有与 echo 包对应的 echo reply 包则认为是状态非法的。对于此类连接,防火墙中的连接信息中的超时时间就要比 TCP 连接信息中的超时时间短得多。通过状态检测,就可以很容易实现你访问别人,而别人不能访问你这种由简单包过滤所不能实现的功能。

8.7 防火墙的发展趋势

随着新的网络技术的出现,防火墙技术呈现以下新的发展。

(1) 目前防火墙在安全性、效率和功能方面的矛盾还是比较突出。防火墙的技术结构,往往是安全性高效率就低,效率高就会以牺牲安全为代价。未来的防火墙要求是高安全性和高效率。使用专门的芯片负责访问控制功能、设计新的防火墙的技术架构是未来防火墙的方向。

(2) 数据加密技术的使用,使合法访问更安全。

(3) 混合使用包过滤技术、代理服务技术和其他一些新技术。

(4) 目前,人们正在设计新的 IP 协议 IPv6(也被称为 IP version 6)。IP 协议的变化将对防火墙的建立与运行产生深刻的影响。

(5) 分布式防火墙。现在的防火墙一般安放在网络的边界,并假设内部网络中的所有主机是可信任的,所有的外部网络主机是不可信任的。但是攻击往往是从内部发起的,所以不是所有的内部主机都是可以信任的,因此提出了分布式防火墙的概念。分布式防火墙是指那些驻留在网络中主机如服务器或台式机并对主机系统自身提供安全防护的软件产品;从广义来讲,分布式防火墙是一种新的防火墙体系结构,它包含如下产品。

① 网络防火墙:即传统的边界防火墙,用于内部网与外部网之间进行访问控制。包括内部网中各个子网之间的防火墙,这种防火墙需支持内部网可能有的非 IP 协议。

② 主机防火墙:对网络中的服务器和台式机进行防护,需要给每一台需要保护的主机安装防火墙,这些主机的物理位置可能在内部网中,也可能在内部网外,如托管服务器或移动办公的便携机。

③ 中心管理:边界防火墙只是网络中的单一设备,管理是单一的。对分布式防火墙来说,每个防火墙作为安全监测机制可以根据安全性的不同要求布置在网络中的任何需要的位置上,但总体安全策略又是统一策划和管理的,安全策略的分发及日志的汇总都是

中心管理应具备的功能。中心管理是分布式防火墙系统的核心和重要特征之一。

(6) 对数据包的全方位的检查。不仅包括数据包头的信息,而且包括数据包的内容信息,查出恶意行为,阻止通过。

8.8　本章小结

防火墙是建立在内外网络边界上的过滤封锁机制,内部网络被认为是安全和可信赖的,而外部网络(通常是 Internet)被认为是不安全和不可信赖的。防火墙的作用是防止不希望的、未经授权的通信进出被保护的内部网络,通过边界控制强化内部网络的安全政策。

防火墙的主要技术有包过滤技术、代理服务器技术、应用网关技术、状态检测包过滤技术,现在最常用的是状态检测包过滤技术。

防火墙的体系结构有双重宿主主机体系结构、被屏蔽主机体系结构和被屏蔽子网体系结构,它们都有各自的优缺点。

堡垒主机位于内部网络的最外层,像堡垒一样对内部网络进行保护。在防火墙体系中,堡垒主机要高度暴露,是在 Internet 上公开的,是网络上最容易遭受非法入侵的设备。所以防火墙设计者和管理人员需要致力于堡垒主机的安全,而且在运行期间对堡垒主机的安全给予特别的注意。堡垒主机应该安装在不传输保密信息的网络上,最好处于一个独立网络,比如 DMZ。

包过滤式的防火墙会检查所有通过的数据包头部的信息,并按照管理员所给定的过滤规则进行过滤。如果对防火墙设定某一内部 IP 地址不能访问某个站点的话,从这个地址来的到某个站点的信息都会被防火墙屏蔽掉。在配置数据包过滤规则之前,需要明确要允许或者拒绝什么服务,并且需要把策略转换成为针对数据包的过滤规则。通过制定数据包过滤规则来控制哪些数据包能够进入或者流出内部网络。

状态检测防火墙对每个合法网络连接保存的信息包括源地址、目的地址、协议类型、协议相关信息(如 TCP/UDP 协议的端口、ICMP 协议的 ID 号)、连接状态(如 TCP 连接状态)和超时时间等,防火墙把这些信息叫做状态。通过状态检测,可实现比简单包过滤防火墙具有更大的安全性。

习　　题

1. 什么是防火墙?防火墙的功能有哪些?
2. 防火墙的体系结构有哪几种?
3. 堡垒主机的构建原则是什么?
4. 过滤规则如何制定?
5. 堡垒主机的日志如何保护?
6. 堡垒主机如何管理?

7. 代理是如何工作的？
8. 状态检测是如何工作的？
9. 复杂协议是如何进行状态检测的？
10. 状态检测有哪些弱点？

第9章

VPN

本章要点:

- VPN的基本概念和特点;
- VPN采用的主要技术;
- 第二层VPN协议的机制和功能;
- 第三层的一种VPN协议的机制和功能。

9.1 VPN概述

9.1.1 VPN的概念

VPN是Virtual Private Network的缩写,是将物理分布在不同地点的网络通过公用骨干网,尤其是Internet连接而成的逻辑上的虚拟子网。为了保障信息的安全,VPN技术采用了鉴别、访问控制、保密性、完整性等措施,以防止信息被泄露、篡改和复制。

V即Virtual,是针对传统的企业"专用网络"而言的。传统的专用网络往往需要建立自己的物理专用线路,使用昂贵的长途拨号以及长途专线服务;而VPN则是利用公共网络资源和设备建立一个逻辑上的专用通道,尽管没有自己的专用线路,但是这个逻辑上的专用通道却可以提供和专用网络同样的功能。换言之,VPN虽然不是物理上真正的专用网络,但却能够实现物理专用网络的功能。

P即Private,表示VPN是被特定企业或用户私有的,并不是任何公共网络上的用户都能够使用已经建立的VPN通道,而是只有经过授权的用户才可以使用。在该通道内传输的数据经过了加密和认证,使得通信内容既不能被第三者修改,又无法被第三者破解,从而保证了传输内容的完整性和机密性。因此,只有特定的企业和用户群体才能够利用该通道进行安全的通信。

N即Network,表示这是一种专门的组网技术和服务,企业为了建立和使用VPN必须购买和配备相应的网络设备。

9.1.2 VPN的类型

VPN有3种类型:Access VPN(远程访问VPN)、Intranet VPN(企业内部VPN)和Extranet VPN(企业扩展VPN),这3种类型的VPN分别对应于传统的远程访问网络、企业内部的Intranet以及企业和合作伙伴的网络所构成的Extranet。

1. Access VPN

Access VPN 即所谓的移动 VPN，适用于企业内部人员流动频繁或远程办公的情况，出差员工或者在家办公的员工利用当地 ISP(Internet Service Provider，Internet 服务提供商)就可以和企业的 VPN 网关建立私有的隧道连接，如图 9-1 所示。

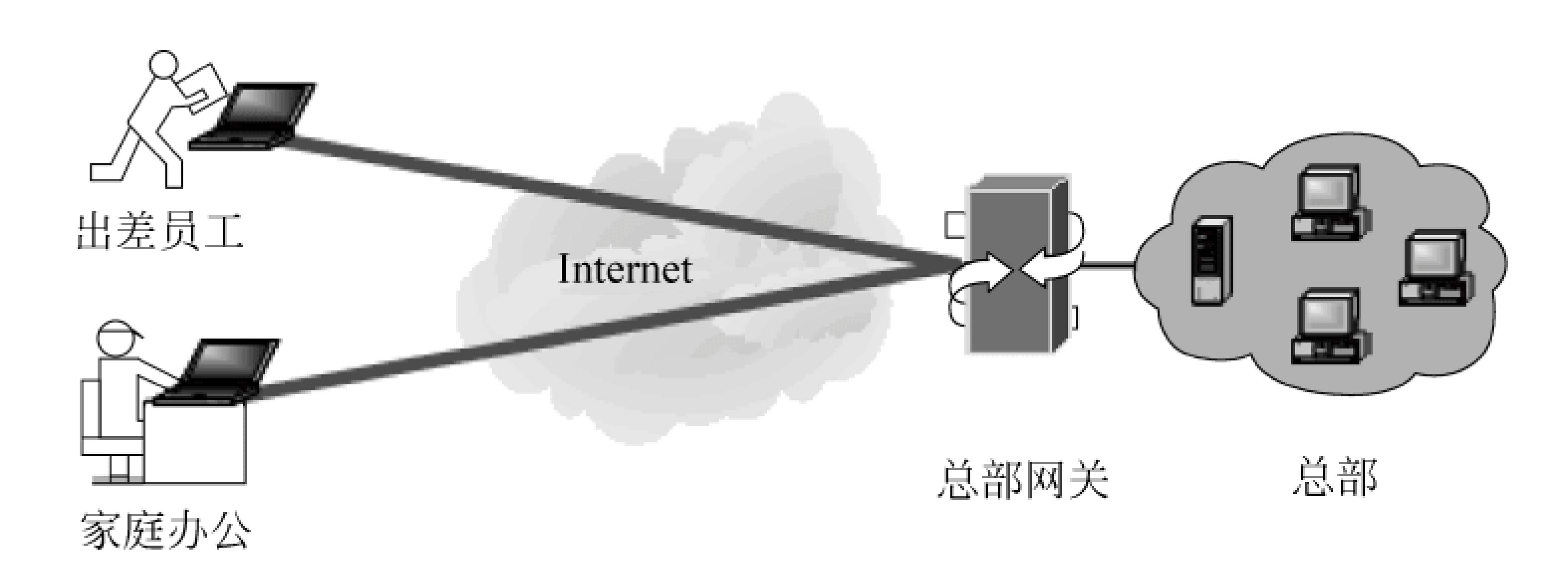


图 9-1　Access VPN

Access VPN 对应于传统的远程访问内部网络。在传统方式中，在企业网络内部需要架设一个拨号服务器作为 RAS(Remote Access Server)，用户通过拨号到该 RAS 来访问企业内部网。这种方式需要购买专门的 RAS 设备，价格昂贵，用户只能进行拨号，也不能保证通信安全，而且对于远程用户可能要支付昂贵的长途拨号费用。

Access VPN 通过拨入当地的 ISP 进入 Internet 再连接企业的 VPN 网关，在用户和 VPN 网关之间建立一个安全的"隧道"，通过该隧道安全地访问远程的内部网，这样既节省了通信费用，又能保证安全性。

Access VPN 的拨入方式包括拨号、ISDN、数字用户线路(xDSL)等，唯一的要求就是能够使用合法 IP 地址访问 Internet，具体何种方式没有关系。通过这些灵活的拨入方式能够让移动用户、远程用户或分支机构安全地接入到内部网络。

2. Intranet VPN

如果要进行企业内部异地分支机构的互联，可以使用 Intranet VPN 方式，这是所谓的网关对网关 VPN，它对应于传统的 Intranet 解决方案，如图 9-2 所示。

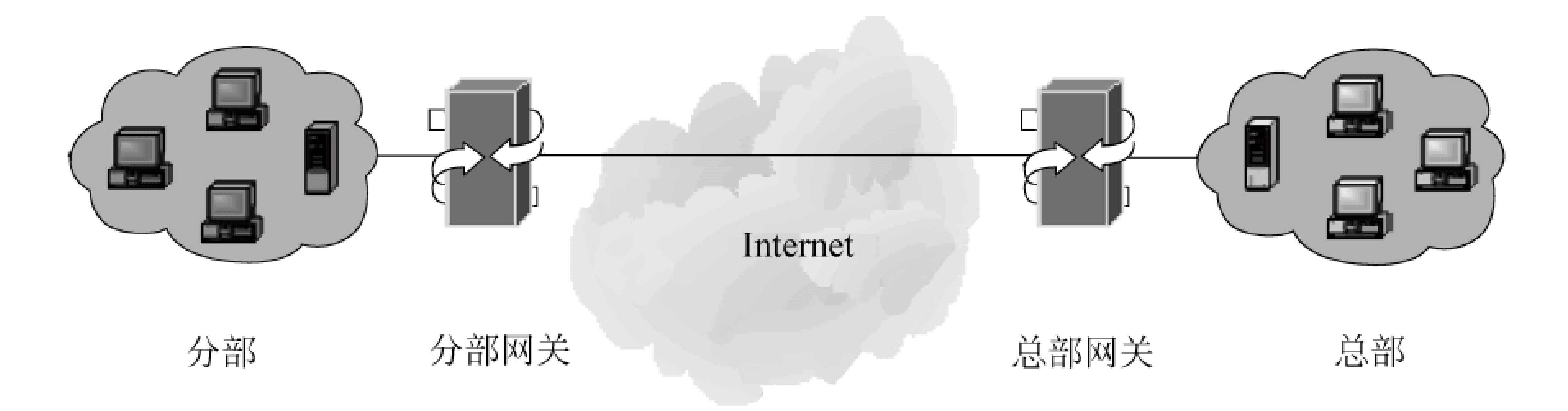


图 9-2　Intranet VPN

Intranet VPN 在异地两个网络的网关之间建立了一个加密的 VPN 隧道，两端的内部网络可以通过该 VPN 隧道安全地进行通信，就好像和本地网络通信一样。

Intranet VPN 利用公共网络(如 Internet)的基础设施，连接企业总部、远程办事处和

分支机构。企业拥有与专用网络相同的策略，包括安全、服务质量(QoS)、可管理性和可靠性。

3. Extranet VPN

如果一个企业希望将客户、供应商、合作伙伴或兴趣群体连接到企业内部网，可以使用 Extranet VPN，它对应于传统的 Extranet 解决方案，如图 9-3 所示。

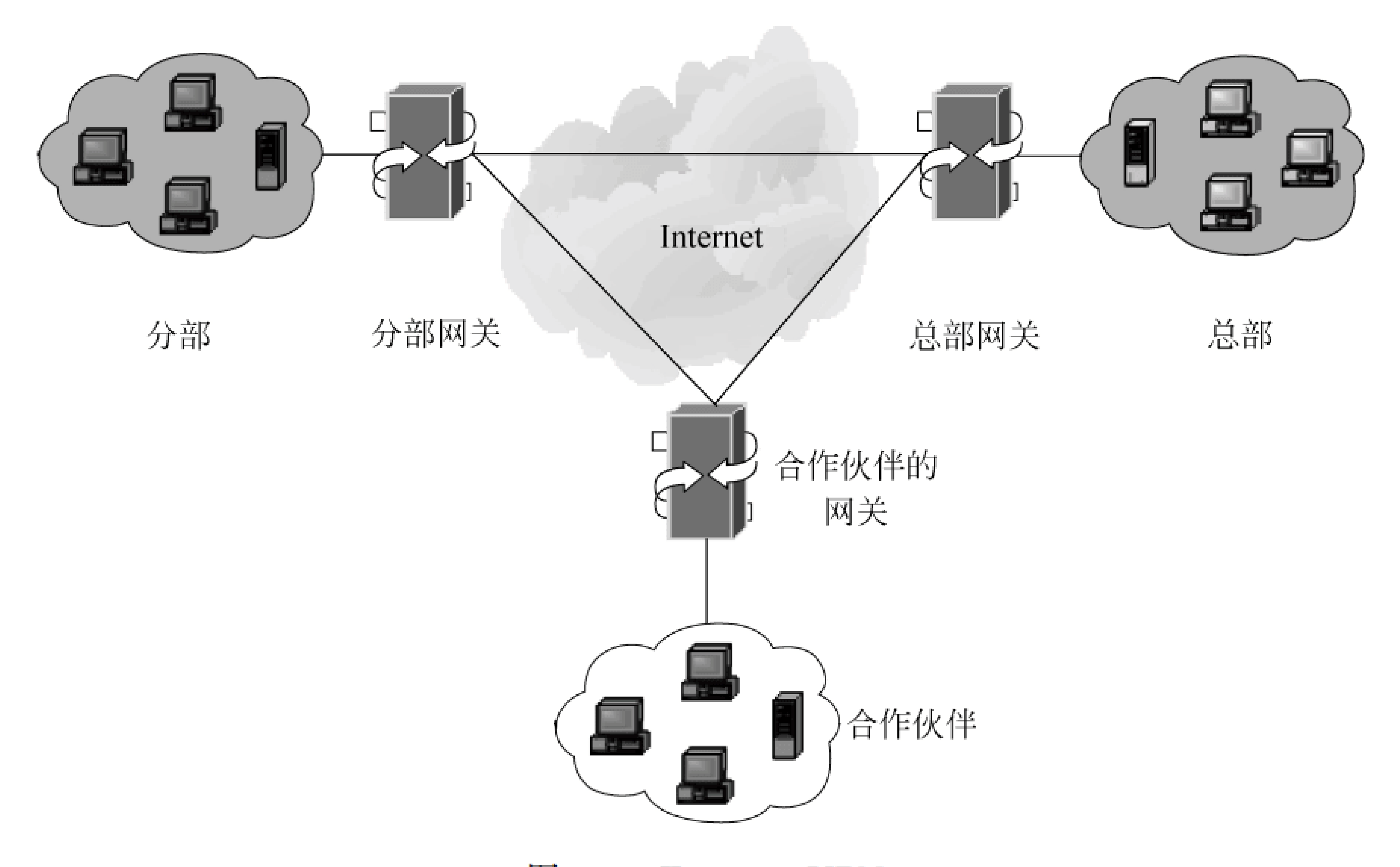


图 9-3　Extranet VPN

Extranet VPN 其实也是一种网关对网关的 VPN，与 Intranet VPN 不同的是，它需要在不同企业的内部网络之间组建，需要有不同协议和设备之间的配合和不同的安全配置。

9.1.3　VPN 的优点

VPN 具有以下优点。

(1) 降低成本

VPN 是利用了现有的 Internet 或其他公共网络的基础设施为用户创建安全隧道，不需要使用专门的线路，如 DDN 和 PSTN，这样就节省了专门线路的租金。如果是采用远程拨号进入内部网络，访问内部资源，还需要支付长途话费；而采用 VPN 技术，只需拨入当地的 ISP 就可以安全地接入内部网络，这样也节省了线路话费。

(2) 易于扩展

如果采用专线连接，实施起来比较困难，在分部增多、内部网络结点越来越多时，网络结构趋于复杂，费用昂贵。如果采用 VPN，只是在结点处架设 VPN 设备，就可以利用 Internet 建立安全连接，如果有新的内部网络想加入安全连接，只需添加一台 VPN 设备，改变相关配置即可。

(3) 保证安全

VPN 技术利用可靠的加密认证技术，在内部网络之间建立隧道，能够保证通信数据

的机密性和完整性，保证信息不被泄露或暴露给未授权的实体，保证信息不被未授权的实体改变、删除或替代。在现在的网络应用中，除了让外部合法用户通过 VPN 访问内部资源外，还需要内部用户方便地访问 Internet，这样可将 VPN 设备和防火墙配合，在保证网络畅通的情况下，尽可能地保证访问安全。

9.2　VPN 技术

9.2.1　密码技术

VPN 利用 Internet 的基础设施传输企业私有的信息，因此传递的数据必须经过加密，从而确保网络上未授权的用户无法读取该信息，因此，可以说密码技术是实现 VPN 的关键核心技术之一。

大体上，密码技术可以分为两类：对称密钥加密和非对称密钥加密。

1. 对称密钥加密

对称密钥加密，也叫做共享密钥加密，是指加密和解密用的密钥是相同的，数据的发送者和接收者拥有共同的单个密钥。当一段数据要传输时，发送者利用密钥将其加密为密文，并在公共信道上传输，接收者收到密文后也要用相同的密钥将其解密成明文。

比较著名的对称密钥加密算法有 DES 及其各种变形，比如 3DES、GDES、New DES 和 DES 的前身 Lucifer、IDEA、Skipjack、RC4、RC5 等。众多算法中最常用的是 DES（Data Encryption Standard）、AES（Advanced Encryption Standard）和 IDEA（International Data Encryption Algorithm）。

由于加密和解密的密钥相同，因此这种加密算法的安全性取决于是否有未经授权的人获得了密钥。一旦密钥泄露，无论该算法在运行时多么复杂，设计多么精良，密文可以轻易地被破解。为了保证密钥的机密性，希望使用对称密钥加密通信的双方，在交换加密数据之前必须先安全地交换密钥。

衡量对称算法优劣的一个重要尺度是其密钥的长度。密钥位数越长，密钥的可能性越多，在找到正确密钥之前必须测试的密钥数量就越多，从而破解这种算法就越困难。另一个指标是看算法是否经得住算法分析的考验，如差分密码分析、线性密码分析等，有的算法的密钥长度虽然很长，但算法有缺陷，可绕过密钥进行破解。

对称密钥加密的优点是运算量小、速度快，适合于加密大量数据的情况；缺点是密钥的管理比较复杂。

2 非对称密钥加密

非对称密钥加密使用两个密钥：一个公钥和一个私钥，这两个密钥在数学上是相关的。这种算法也叫做公钥加密。公钥可以不受保护，可在通信双方之间公开传递，或在公共网络上发布，但相关的私钥是保密的。利用公钥加密的数据只有使用私钥才能解密；利用私钥加密的数据只有使用公钥才能解密。

比较著名的非对称算法有 RSA、背包密码、McEliece 密码、Diffie-Hellman、Rabin、椭圆曲线、ElGamal 算法等。其中最有影响的是 RSA 算法，它能抵抗到目前为止已知的所有密码攻击。

非对称算法采用复杂的数学处理，密钥大小比对称算法的大，它们要求更多的处理器资源，因此其速度较慢。非对称算法不适合加密大量数据的情况，而是经常用于关键数据的加密，比如对称密钥在密钥分发时采用非对称算法。另外非对称加密算法和散列算法结合使用，可以生成数字签名。

非对称密钥加密的优点是解决了对称加密中的密钥交换的困难，密钥管理简单，安全性高；缺点是计算速度相对较慢。因此非对称密钥加密更多用于密钥交换、数字签名、身份认证等，一般不用于对具体信息加密。

一般来说，在 VPN 实现中，双方大量的通信流量的加密使用对称加密算法，而在管理、分发对称加密的密钥上采用更加安全的非对称加密技术。

9.2.2 身份认证技术

VPN 需要解决的首要问题就是网络上用户与设备的身份认证，如果没有一个万无一失的身份认证方案，不管其他安全设施有多严密，整个 VPN 的功能都将失效。

从技术上说，身份认证基本上可以分为两类：非 PKI 体系和 PKI 体系的身份认证。非 PKI 体系的身份认证基本上采用的是 UID+PASSWORD 模式，举例如下：

- PAP，Password Authentication Protocol，口令认证协议；
- CHAP，Challenge-Handshake Authentication Protocol，询问握手认证协议；
- EAP，Extensible Authentication Protocol，扩展身份认证协议；
- MS-CHAP，Microsoft Challenge Handshake Authentication Protocol，微软询问握手认证协议；
- SPAP，Shiva Password Authentication Protocol，Shiva 口令字认证协议；
- RADIUS，Remote Authentication Dial In User Service，远程认定拨号用户服务。

PKI 体系的身份认证的例子有电子商务中用到的 SSL 安全通信协议的身份认证、Kerberos 等。目前常用的方法是依赖于 CA（Certificate Authority，数字证书签发中心）所签发的符合 X.509 规范的标准数字证书。通信双方交换数据前，需先确认彼此的身份，交换彼此的数字证书，双方将此证书进行比较，只有比较结果正确，双方才开始交换数据；否则，不能进行后续通信。

9.2.3 隧道技术

隧道技术通过对数据进行封装，在公共网络上建立一条数据通道（隧道），让数据包通过这条隧道传输。生成隧道的协议有两种：第二层隧道协议和第三层隧道协议。

（1）第二层隧道协议是在数据链路层进行的，先把各种网络协议封装到 PPP 包中，再把整个数据包装入隧道协议中，这种经过两层封装的数据包由第二层协议进行传输。第二层隧道协议有以下几种：

- L2F（RFC 2341，Layer 2 Forwarding）；

- PPTP(RFC 2637,Point-to-Point Tunneling Protocol);
- L2TP(RFC 2661,Layer Two Tunneling Protocol)。

(2) 第三层隧道协议是在网络层进行的,把各种网络协议直接装入隧道协议中,形成的数据包依靠第三层协议进行传输。第三层隧道协议有以下几种:

- IPSec(IP Security),是目前最常用的 VPN 解决方案;
- GRE(RFC 2784,General Routing Encapsulation)。

9.2.4 密钥管理技术

在 VPN 应用中密钥的分发与管理非常重要。密钥的分发有两种方法:一种是通过手工配置的方式,另一种是采用密钥交换协议动态分发。手工配置的方法要求密钥更新不要太频繁,否则管理工作量太大,因此只适合于简单网络的情况。密钥交换协议采用软件方式动态生成密钥,保证密钥在公共网络上安全地传输而不被窃取,适合于复杂网络的情况,而且密钥可快速更新,可以显著提高 VPN 应用的安全性。目前主要的密钥交换与管理标准有 SKIP(Simple Key Management for IP)和 ISAKMP(Internet Security Association and Key Management Protocol,Internet 安全联盟和密钥管理协议,RFC2408)/Oakley(RFC2412)。

SKIP 是由 SUN 所发展的技术,主要利用 Diffie-Hellman 算法在网络上传输密钥。在 ISAKMP/Oakley 中,Oakley 定义如何辨认及确认密钥,ISAKMP 定义分配密钥的方法。

9.3 第二层隧道协议——L2F、PPTP 和 L2TP

第二层隧道协议用于传输第二层网络协议,它主要应用于构建 Access VPN。第二层隧道协议主要有 3 种:一种是由 Cisco、Nortel 等公司支持的 L2F 协议,Cisco 路由器中支持此协议;另一种是 Microsoft、Ascend、3COM 等公司支持的 PPTP 协议,Windows NT 4.0以上版本中支持此协议;而成为二层隧道协议工业标准的是由 IETF 起草并由 Microsoft、Ascend、Cisco、3COM 等公司参与制定的 L2TP 协议,它结合了上述两个协议的优点。这一节分别讨论这 3 个协议。

在具体讨论协议之前,先看一下隧道技术中的几个基本概念。

9.3.1 隧道协议的基本概念

无论何种隧道协议,其数据包格式都是由乘客协议、封装协议和传输协议 3 部分组成的。下面 以 L2TP 为例,如图 9-4 所示,看一下隧道协议的组成。

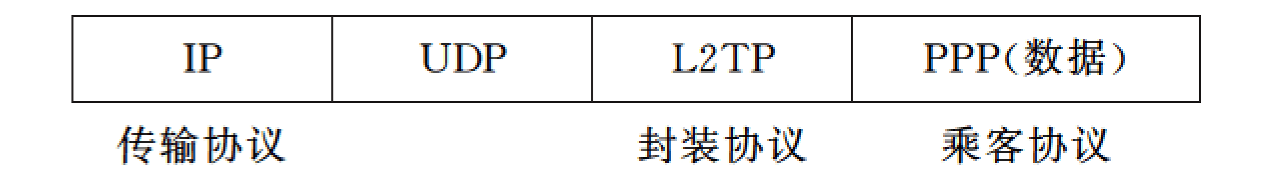


图 9-4 隧道协议的封装

(1) 乘客协议:乘客协议是指用户要传输的数据,也就是被封装的数据,它们可以是 IP、PPP、SLIP 等。这是用户真正要传输的数据,如果是 IP 协议,其中包含的地址有可能是保留 IP 地址。

(2) 封装协议:封装协议用于建立、保持和拆卸隧道。即将讨论的 L2F、PPTP、L2TP、GRE 就属于封装协议。

(3) 传输协议:乘客协议被封装之后应用传输协议,图 9-4 中使用 UDP 协议对 L2TP 协议数据包进行了封装。

为了理解隧道,不妨用邮政系统打个比方。乘客协议就是我们写的信,信的语言可以是汉语、英语、法语等,具体如何解释由写信人、读信人自己负责,这就对应于多种乘客协议,对乘客协议数据的解释由隧道双方负责。封装协议就是信封,可能是平信、挂号或者是 EMS,这对应于多种封装协议,每种封装协议的功能和安全级别有所不同。传输协议就是信的运输方式,可以是陆运、海运或者空运,这对应于不同的传输协议。

根据隧道的端点是用户计算机还是拨号接入服务器,隧道可以分为两种:自愿隧道(Voluntary Tunnel)和强制隧道(Compulsory Tunnel)。

1. 自愿隧道

客户端计算机可以通过发送 VPN 请求来配置和创建一条自愿隧道,此时用户端计算机作为隧道的客户方成为隧道的一个端点。为了创建自愿隧道,工作站或路由器上必须安装隧道客户软件,并创建到目标隧道服务器的虚拟连接。目前,自愿隧道是最普遍使用的隧道类型。

创建自愿隧道的前提是客户端和服务器之间要有一条 IP 连接(通过局域网或拨号线路)。使用拨号方式时,客户端必须在建立隧道之前创建与 Internet 的拨号连接。一个最典型的例子是 Internet 拨号用户必须在创建 Internet 隧道之前拨通本地 ISP,以取得与 Internet 的连接。

一种误解认为 VPN 只能使用拨号连接,其实,建立 VPN 只要求 IP 网络的支持即可。一些客户机(如家用 PC)可以通过使用拨号方式连接 Internet 建立 IP 传输,这只是为创建隧道所做的初步准备,本身并不属于隧道协议。

2 强制隧道

强制隧道由支持 VPN 的拨号接入服务器来配置和创建。此时,用户端的计算机不作为隧道端点,而是由位于客户计算机和隧道服务器之间的拨号接入服务器作为隧道客户端,成为隧道的一个端点。

能够代替客户端计算机来创建隧道的网络设备包括支持 PPTP 协议的 FEP(Front-End Processor,前端处理器)、支持 L2TP 协议的 LAC(L2TP Access Concentrator,L2TP 接入集中器)或支持 IPSec 的安全 IP 网关。为正常地发挥功能,FEP 必须安装适当的隧道协议,同时必须能够在客户计算机建立起连接时创建隧道。

以 Internet 为例,客户机向位于本地 ISP 的能够提供隧道技术的 NAS(Network Access Server)发出拨号呼叫,例如,企业可以与某个 ISP 签订协议,由 ISP 为企业在全国范围内设置一套 FEP,这些 FEP 可以通过 Internet 创建一条到隧道服务器的隧道,隧道

服务器与企业的专用网络相连。这样,就可以将不同地方合并成企业网络端的一条单一的 Internet 连接。

因为客户只能使用由 FEP 创建的隧道,所以称为强制隧道。一旦最初的连接成功,所有客户端的数据流将自动通过隧道发送。使用强制隧道,客户端计算机建立单一的 PPP 连接,当客户拨入 NAS 时,一条隧道将被创建,所有的数据流自动通过该隧道路由。可以配置 FEP 为所有的拨号客户创建到指定隧道服务器的隧道,也可以配置 FEP 基于不同的用户名或目的地创建不同的隧道。

自愿隧道技术为每个客户创建独立的隧道,而强制隧道中 FEP 和隧道服务器之间建立的隧道可以被多个拨号客户共享,而不必为每个客户建立一条新的隧道。因此,一条隧道中可能会传递多个客户的数据信息,只有在最后一个隧道用户断开连接之后才终止整条隧道。

9.3.2　L2F

L2F(Layer Two Forwarding Protocol,二层转发协议)是由 Cisco 公司提出的隧道技术,可以支持多种传输协议,如 IP、ATM、帧中继。

首先,远端用户通过任何拨号方式接入公共 IP 网络,例如,按常规方式拨号到 ISP 的 NAS,建立 PPP 连接;然后,NAS 根据用户名等信息,发起第二重连接,通向企业的本地 L2F 网关服务器,这个 L2F 服务器把数据包解包之后发送到企业内部网上。

在 L2F 中,隧道的配置和建立对用户是完全透明的,L2F 没有确定的客户方。

9.3.3　PPTP

PPTP(Point-to-Point Tunneling Protocol,点到点隧道协议)在 RFC 2637 中定义,该协议将 PPP 数据包封装在 IP 数据包内通过 IP 网络(如 Internet 或 Intranet)进行传送。PPTP 协议可看作 PPP 协议的一种扩展,它提供了一种在 Internet 上建立多协议的 VPN 的通信方式,远端用户能够通过任何支持 PPTP 的 ISP 访问公司的专用网络。

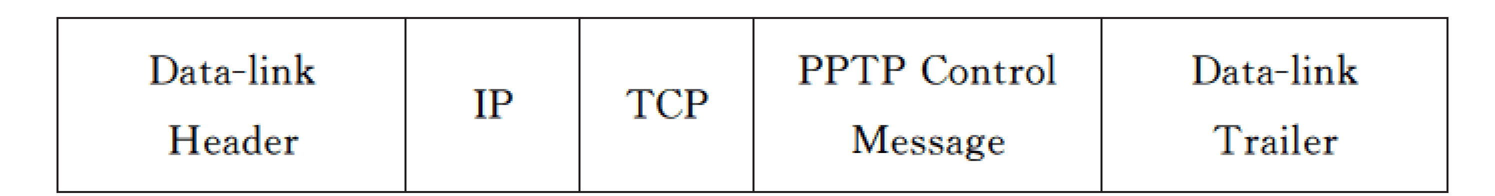
PPTP 协议提供了 PPTP 客户端和 PPTP 服务器之间的加密通信。PPTP 客户端是指运行了 PPTP 协议的 PC,如支持该协议的 Windows 客户机;PPTP 服务器是指运行该协议的服务器,如支持该协议的 Windows NT 服务器。PPTP 客户端和服务器进行 VPN 通信的前提是两者之间有连通且可用的 IP 网络,也就是说 PPTP 客户端必须能够通过 IP 网络访问 PPTP 服务器。如果 PPTP 客户端是通过拨号上网,则要先拨号到本地的 ISP 建立 PPP 连接,从而可以访问 Internet。如果 PPTP 客户端直接连接到 IP 网络,即可直接通过该 IP 网络与 PPTP 服务器取得连接。

PPTP 客户端和服务器之间的报文有两种:控制报文负责 PPTP 隧道的建立、维护和断开;数据报文负责传输用户的真正数据。

1. 控制报文

PPTP 客户端"拨号"到 PPTP 服务器创建 PPTP 隧道,这里的"拨号"并不是拨服务器的电话号码,而是连接 PPTP 服务器的 TCP 1723 端口建立控制连接。控制连接负责隧道的建立、维护和断开。PPTP 控制连接携带 PPTP 呼叫控制和管理信息,用于维护

PPTP 隧道，其中包括周期性地发送回送请求和回送应答报文，以期检测出客户机与服务器之间可能出现的连接中断。PPTP 控制连接数据包包括一个 IP 报头、一个 TCP 报头和 PPTP 控制信息，如图 9-5 所示。



Data-link Header	IP	TCP	PPTP Control Message	Data-link Trailer

图 9-5　PPTP 控制报文

在创建基于 PPTP 的 VPN 连接过程中，使用的认证机制与创建 PPP 连接时相同。此类认证机制主要有 EAP、MS-CHAP、CHAP、SPAP 和 PAP。

PPTP 继承 PPP 有效载荷的加密和压缩。在 Windows 2000 中，由于 PPP 帧使用 MPPE(Microsoft Point-to-Point Encryption，微软点对点加密技术)进行加密，因此认证机制必须采用 EAP 或 MS-CHAP。

2 数据报文

在隧道建好之后，真正的用户数据经过加密和/或压缩之后，再依次经过 PPP、GRE、IP 的封装最终得到一个 IP 包，如图 9-6 所示，通过 IP 网络发送到 PPTP 服务器；PPTP 服务器收到该 IP 后层层解包，得到真正的用户数据，并将用户数据转发到内部网络上。用户的数据可以是多种协议，比如 IP 数据包、IPX 数据包或者 NetBEUI 数据包。PPTP 采用 RSA 公司的 RC4 作为数据加密算法，保证了隧道通信的安全性。

Data-link Header	IP Header	GRE Header	PPP Header	Encrypted PPP Payload (IP Datagram, IPX Datagram, NetBEUI Frame)	Data-link Trailer

图 9-6　PPTP 数据报文

与 L2F 相比，PPTP 把建立隧道的主动权交给了用户，但用户需要在其 PC 机上配置 PPTP，这样不仅增加了用户的工作量，而且造成网络的安全隐患。另外，PPTP 只支持 IP 作为其传输协议。

9.3.4　L2TP

L2TP(Layer Two Tunneling Protocol，第二层隧道协议)由 RFC 2661 定义，它结合了 L2F 和 PPTP 的优点，可以让用户从客户端或访问服务器端发起 VPN 连接。L2TP 是由 Cisco、Ascend、Microsoft 等公司在 1999 年联合制定的，已经成为二层隧道协议的工业标准，并得到了众多网络厂商的支持。

L2TP 协议支持 IP、X. 25、帧中继或 ATM 等作为传输协议，但目前仅定义了基于 IP 网络的 L2TP。L2TP 隧道协议可用于 Internet，也可用于其他企业专用 Intranet 中。

L2TP 客户端是使用 L2TP 隧道协议和 IPSec 安全协议的 VPN 客户端，而 L2TP 服务器是使用 L2TP 隧道协议和 IPSec 安全协议的 VPN 服务器。客户端和服务器进行 VPN 通信的前提是两者之间有连通且可用的 IP 网络，也就是说，L2TP 客户端必须可以通过 IP 网络访问 L2TP 服务器。如果 L2TP 客户端是通过拨号上网，则要先拨号到本地

的 ISP 建立 PPP 连接，从而访问 Internet。如果 L2TP 客户端直接连接到 IP 网络，即可直接通过该 IP 网络与 L2TP 服务器取得连接。

在介绍 L2TP 客户端和服务器之间通信的整个流程之前，需要首先了解下列术语。

(1) LAC：L2TP Access Concentrator，L2TP 访问集中器，是附属在交换网络上的具有 PPP 端系统和 L2TP 协议处理能力的设备，LAC 一般就是一个 NAS(Network Access Server，网络接入服务器)，它为用户通过 PSTN/ISDN 提供网络接入服务。

(2) LNS：L2TP Network Server，L2TP 网络服务器，是 PPP 端系统上用于处理 L2TP 协议服务器端部分的软件。

L2TP 主要由 LAC 和 LNS 构成，LAC 支持客户端的 L2TP，它用于发起呼叫，接收呼叫和建立隧道；LNS 是所有隧道的终点。在传统的 PPP 连接中，用户拨号连接的终点是 LAC，L2TP 使得 PPP 协议的终点延伸到 LNS。

L2TP 隧道的建立过程如图 9-7 所示，具体描述如下。

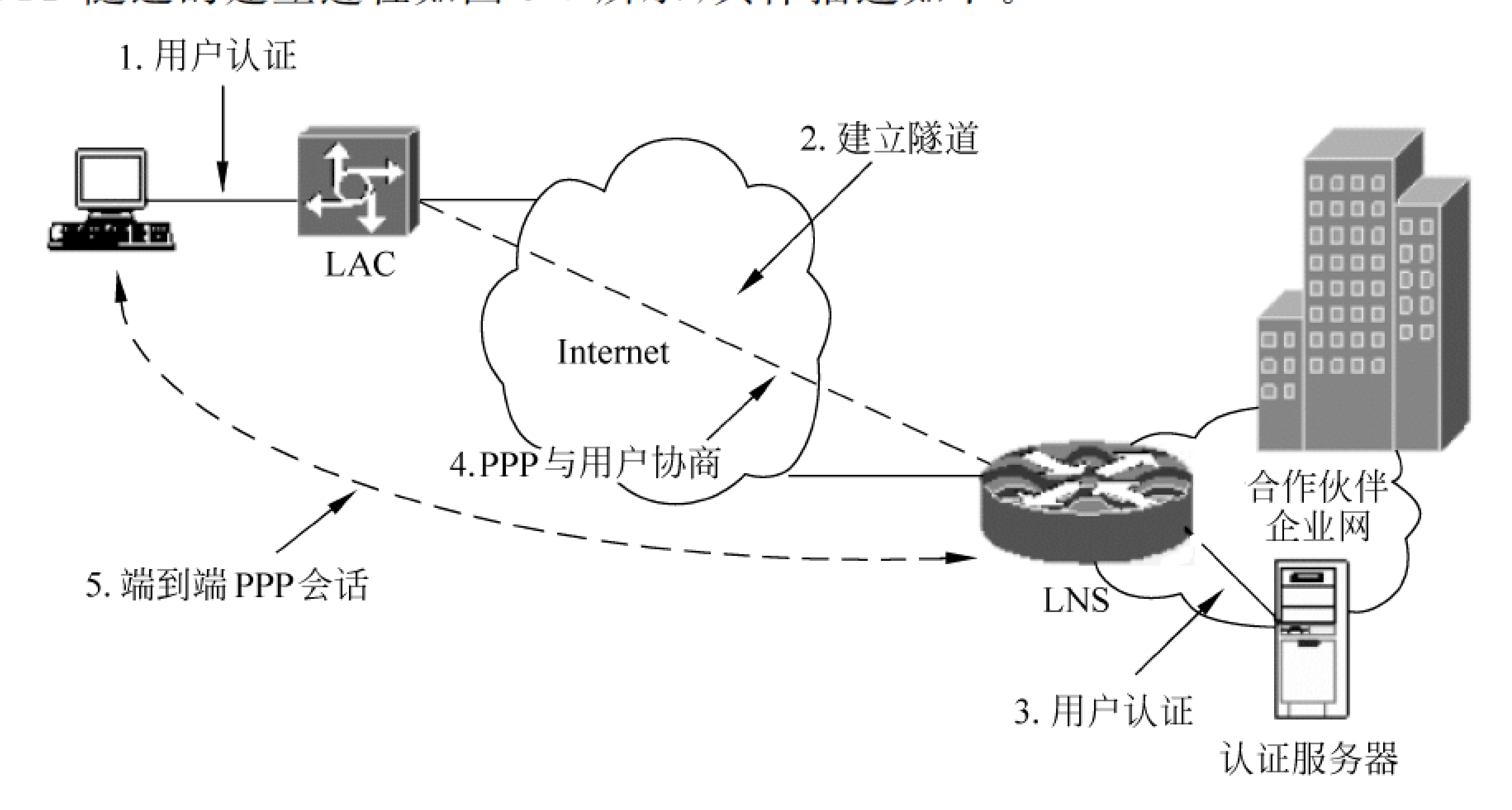


图 9-7　L2TP 的连接过程

(1) 用户通过 PSTN/ISDN 拨号至本地的接入服务器 LAC；LAC 接收呼叫并进行基本的辨别，这一过程可以采用几种标准，如使用域名识别、呼叫线路识别(CLID)或拨号 ID 业务(DNIS)等。

(2) 当用户被确认为合法企业用户时，就建立一个通向 LNS 的拨号 VPN 隧道。

(3) 企业内部的安全服务器如 TACACS+、RADIUS 鉴定拨号用户。

(4) LNS 与远程用户交换 PPP 信息，分配 IP 地址。LNS 可采用企业专用地址(未注册的 IP 地址)或服务提供商提供的地址空间分配 IP 地址。因为内部源 IP 地址与目的地 IP 地址实际上都通过服务提供商的 IP 网络在 PPP 信息包内传送，企业专用地址对提供者的网络是透明的。

(5) 端到端的数据从拨号用户传到 LNS。在实际应用中，LAC 将拨号用户的 PPP 帧封装后，传送到 LNS，LNS 去掉封装包头，得到 PPP 帧，再去掉 PPP 帧头，得到网络层数据包。

L2TP 客户端和服务器之间的报文也有两种：控制报文和数据报文。不过这两种报文均采用 UDP 协议封装和传送 PPP 帧。PPP 帧的有效载荷即用户传输数据，可以经过

加密和/或压缩。但需要指出的是，与 PPTP 不同，在 Windows 2000 中，L2TP 客户机不采用 MPPE 对 L2TP 连接进行加密，L2TP 连接加密由 IPSec ESP 提供。

1. 控制报文

控制报文用于隧道的建立与维护。与 PPTP 不同，L2TP 不是通过 TCP 协议来进行隧道维护，而是采用 UDP 协议。在 Windows 2000 中，L2TP 客户端和服务器都使用 UDP 1701 端口，不过 Windows 2000 L2TP 服务器也支持客户端使用非 1701 UDP 端口，UDP 封装报文结构如图 9-8 所示。

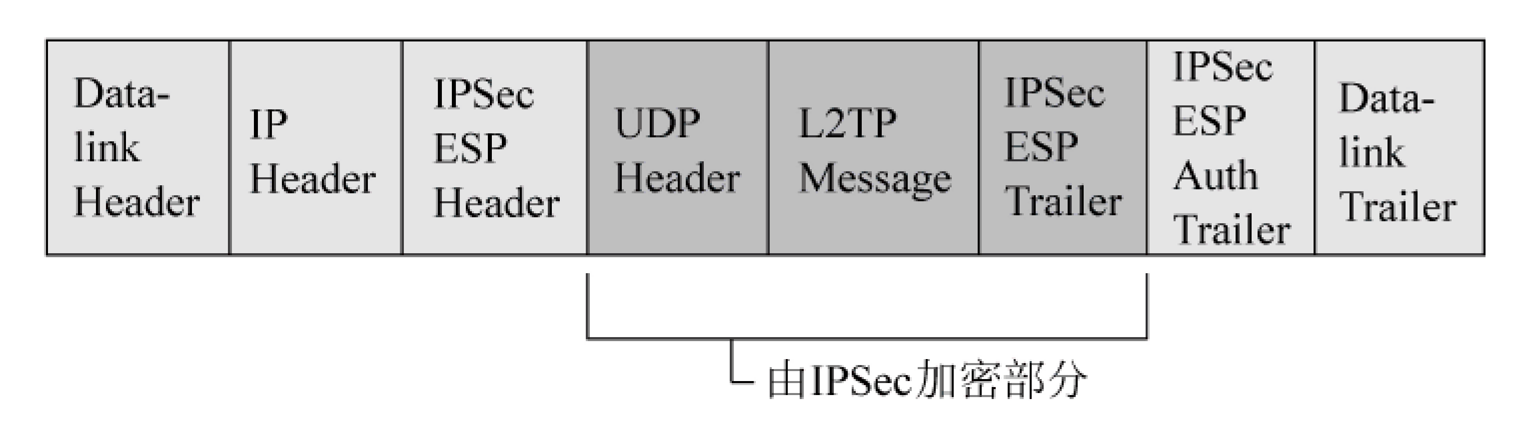


图 9-8　L2TP 控制报文

在 Windows 2000 实现中，L2TP 控制报文即 UDP 数据报经过 IPSec ESP 的加密。

由于 UDP 提供的是无连接的数据包服务，因此 L2TP 采用将报文序列化的方式来保证 L2TP 报文的按序递交。在 L2TP 控制报文中，Next-Received 字段（类似于 TCP 中的确认字段）和 Next-Sent 字段（类似于 TCP 中的序列号字段）用于维持控制报文的序列化，无序数据包将被丢弃。Next-Received 字段和 Next-Sent 字段同样用于用户传输数据的按序递交和流控制。L2TP 控制报文的确切格式，请参阅 L2TP Internet 草案。

L2TP 支持一条隧道内的多路呼叫。在 L2TP 的控制报文以及 L2TP 数据帧的报头内，Tunnel ID 标识了一条隧道而 Call ID 标识了该隧道内的一路呼叫。

在 Windows 2000 中，创建一条未经 IPSec 加密的 L2TP 连接是有可能的，但在这种情形下，由于用户私有数据没有经过加密处理，因此该 L2TP 连接不属于 VPN 连接。非加密 L2TP 连接一般临时性地对基于 IPSec 的 L2TP 连接进行故障诊断和排除，在这种情况下，可以省略 IPSec 认证和协商过程。

创建 L2TP 隧道时必须使用与 PPP 连接相同的认证机制，诸如 EAP、MS-CHAP、CHAP、SPAP 和 PAP。基于 Internet 的 L2TP 服务器即使用 L2TP 协议的拨号服务器，它的一个接口在外部网络 Internet 上，另一个接口在目标专用网络 Intranet 上。

2 数据报文

L2TP 隧道维护控制报文和隧道化用户传输数据具有相同的包格式。

L2TP 用户传输数据的隧道化过程采用多层封装的方法。图 9-9 显示了封装后在隧道中传输的基于 IPSec 的 L2TP 数据包格式。

数据发送端的发送处理过程如下：

（1）L2TP 封装。初始 PPP 有效载荷如 IP 数据报、IPX 数据报或 NetBEUI 帧等首先经过 PPP 报头和 L2TP 报头的封装。

（2）UDP 封装。L2TP 帧进一步添加 UDP 报头进行 UDP 封装，在 UDP 报头中，源

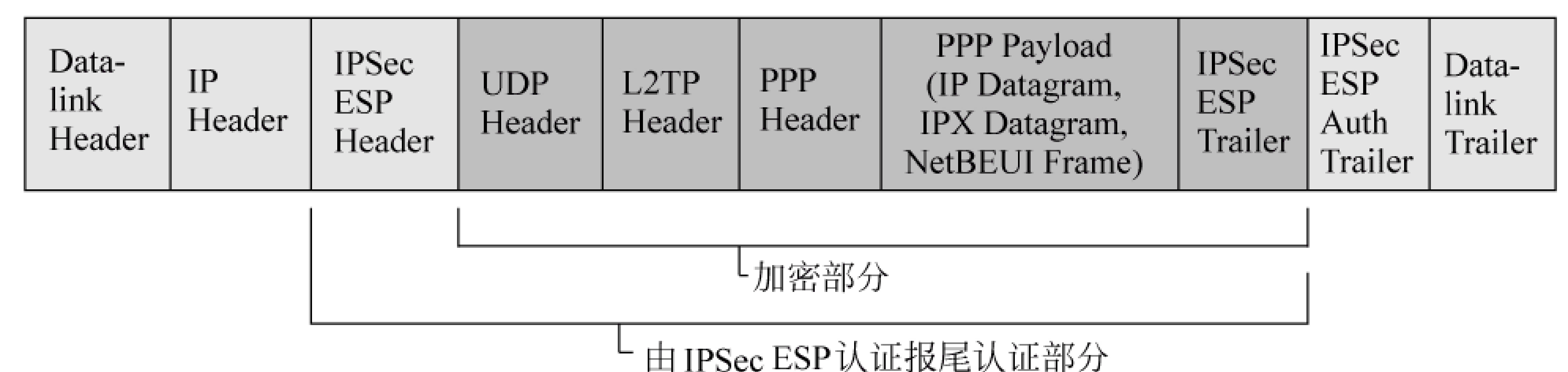


图 9-9　L2TP 数据报文

端和目的端端口号均设置为 1701。

(3) IPSec 封装。基于 IPSec 安全策略，UDP 报文通过添加 IPSec 封装安全负载 ESP 报头、报尾和 IPSec 认证报尾，进行 IPSec 加密封装。

(4) IP 封装。在 IPSec 数据报外再添加 IP 报头进行 IP 封装，IP 报头中包含 VPN 客户机和服务器的源端和目的端 IP 地址。

(5) 数据链路层封装。数据链路层封装是 L2TP 帧多层封装的最后一层，依据不同的物理网络再添加相应的数据链路层报头和报尾。例如，如果 L2TP 帧将在以太网上传输，则用以太网报头和报尾对 L2TP 帧进行数据链路层封装；如果 L2TP 帧将在点对点 WAN 上传输，如模拟电话网或 ISDN 等，则用 PPP 报头和报尾对 L2TP 帧进行数据链路层封装。

数据接收端的处理过程如下：

(1) 处理并去除数据链路层报头和报尾。

(2) 处理并去除 IP 报头。

(3) 用 IPSec ESP 认证报尾对 IP 有效载荷和 IPSec ESP 报头进行认证。

(4) 用 IPSec ESP 报头对数据报的加密部分进行解密。

(5) 处理 UDP 报头并将数据报提交给 L2TP 协议。

(6) L2TP 协议依据 L2TP 报头中 Tunnel ID 和 Call ID 分解出某条特定的 L2TP 隧道。

(7) 依据 PPP 报头分解出 PPP 有效载荷，并将它转发至相关的协议驱动程序做进一步处理。

9.3.5　PPTP 和 L2TP 的比较

PPTP 和 L2TP 都使用 PPP 协议对数据进行封装，然后添加附加包头用于数据在互联网络上的传输。尽管两个协议非常相似，但是仍存在以下几方面的不同：

(1) PPTP 要求互联网络为 IP 网络，L2TP 只要求隧道媒介提供面向数据包的点对点的连接。L2TP 可以在 IP(使用 UDP)、帧中继永久虚拟电路(PVCs)、X. 25 虚拟电路(VCs)或 ATM VCs 网络上使用。

(2) PPTP 只能在两端点间建立单一隧道。L2TP 支持在两端点间使用多隧道。使用 L2TP，用户可以针对不同的服务质量创建不同的隧道。

(3) L2TP 可以提供包头压缩。当压缩包头时，系统开销占用 4 个字节，而 PPTP 协

议下要占用 6 个字节。

(4) L2TP 可以提供隧道验证，而 PPTP 则不支持隧道验证。但是当 L2TP 或 PPTP 与 IPSec 共同使用时，可以由 IPSec 提供隧道验证，而不需要在第二层协议上验证隧道。

9.4　第三层隧道协议——GRE

第三层隧道协议用于传输第三层网络协议。其实第三层隧道协议并不是一项很新的技术，早在 1994 年就出现的 GRE(RFC 1701)协议就是一个第三层隧道协议。由 IETF 制定的新一代 Internet 安全标准 IPSec 协议也是第三层隧道协议。在本节中，我们讨论 GRE 协议，IPSec 协议将在下一章中专门讨论。

GRE(Generic Routing Encapsulation，通用路由封装协议)由 Cisco 和 NetSmiths 公司于 1994 年提交给 IETF，标号为 RFC 1701 和 RFC 1702。在 2000 年，Cisco 等公司又对 GRE 协议进行了修订，称为 GRE V2，标号为 RFC 2784。

GRE 是通用的路由封装协议，支持全部的路由协议(如 RIP2、OSPF 等)，用于在 IP 包中封装任何协议的数据包，包括 IP、IPX、NetBEUI、AppleTalk、Banyan VINES、DECnet 等。在 GRE 中，乘客协议就是上面这些被封装的协议，封装协议就是 GRE，传输协议就是 IP。GRE 与 IP in IP、IPX over IP 等封装形式很相似，但比它们更通用。在 GRE 的处理中，很多协议的细微差异都被忽略，这使得 GRE 不限于某个特定的“X over Y”应用，而是一种通用的封装形式。

具体地说，路由器接收到一个需要封装和路由的原始数据包(如IP包)，先在这个数据包的外面增加一个 GRE 头部构成 GRE 报文，再为 GRE 报文增加一个 IP 头，从而构成最终的 IP 包。这个新生成的 IP 包完全由 IP 层负责转发，中间的路由器只负责转发，而根本不关心是何种乘客协议。以乘客协议 IP 为例，GRE 封装过程如图 9-10 所示。



IP 头部
GRE 头部
原始 IP 数据包

图 9-10　GRE 报文

利用 GRE 来进行 VPN 通信的原理如图 9-11 所示。

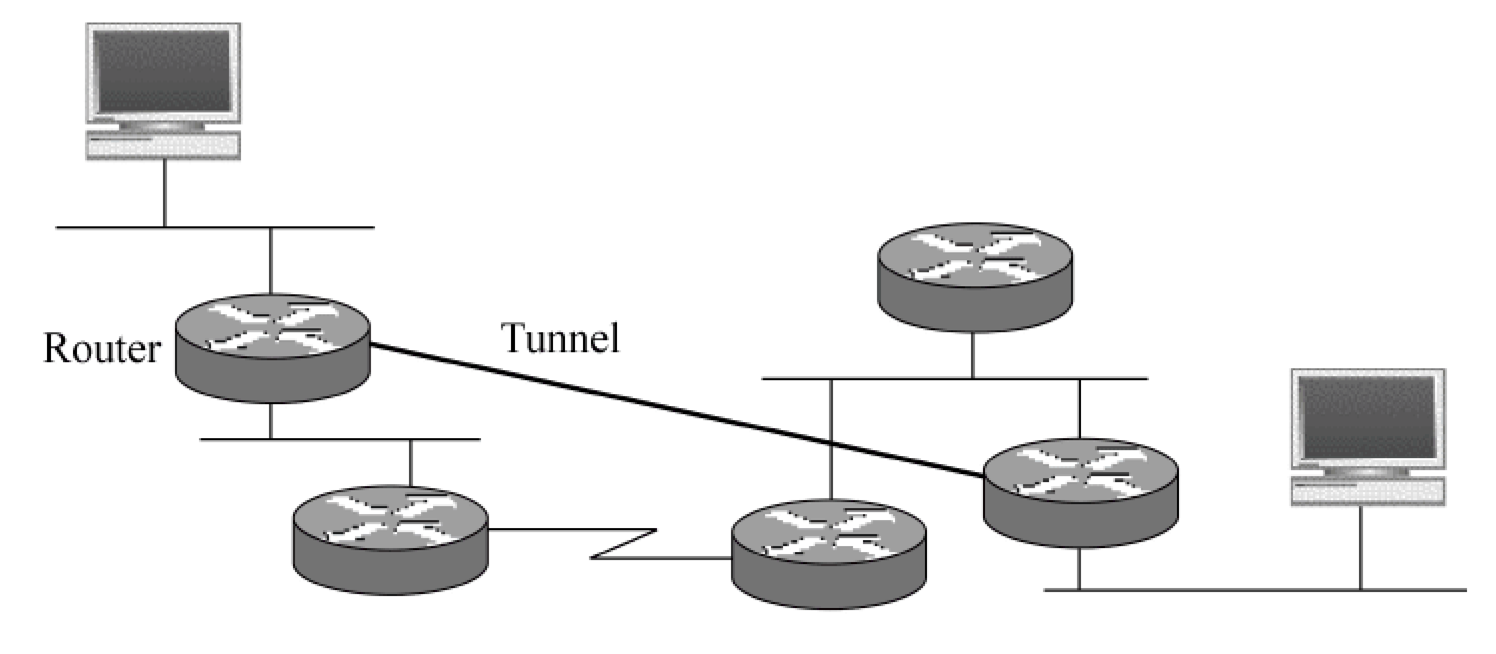


图 9-11　利用 GRE 实现 VPN

因为企业私有网络的 IP 地址通常是自行规划的保留 IP 地址，只是在企业网络出口有一个公网 IP 地址。原始 IP 包的 IP 地址通常是企业私有网络规划的保留 IP 地址，而外层的 IP 地址是企业网络出口的 IP 地址，因此，尽管私有网络的 IP 地址无法和外部网络进行正确的路由，但这个封装之后的 IP 包可以在 Internet 上路由。在接收端，将收到的包的 IP 头部和 GRE 头部解开后，将原始的 IP 数据包发送到自己的私有网络上，此时在私有网络上传输的 IP 包的地址是保留 IP 地址，从而可以访问到远程企业的私有网络。这种技术是最简单的 VPN 技术。

GRE 协议有如下优点：

(1) 通过 GRE，用户可以利用公共 IP 网络连接非 IP 网络，如 IPX 网络、AppleTalk 网络等。多协议的本地网可以通过单一协议的骨干网实现传输，比如两端的私有网络既有 IP 网又有 IPX 等其他网络，通过 GRE，可以使所有协议的私有网络连接起来。

(2) 通过 GRE，还可以使用保留地址进行网络互联，或者对公网隐藏企业网的 IP 地址。

(3) 扩大了网络的工作范围，包括那些路由网关有限的协议。如 IPX 包最多可以转发 16 次(即经过 16 个路由器)，而在一个隧道连接中看上去只经过一个路由器。

(4) GRE 只提供封装，不提供加密，对路由器的性能影响较小，设备档次要求相对较低。

不过，由于 GRE 协议提出较早，也存在着如下的一些缺点：

(1) GRE 只提供了数据包的封装，而没有加密功能来防止网络监听和攻击，所以在实际环境中经常与 IPSec 一起使用。由 IPSec 提供用户数据的加密，从而给用户提供更好的安全性。

(2) 由于 GRE 与 IPSec 采用的是同样的基于隧道的 VPN 实现方式，所以 IPSec VPN 在管理、组网上的缺陷，GRE VPN 也同样具有。

(3) 同时由于对原有 IP 报文进行了重新封装，所以同样无法实施 IP QoS 策略。

综合上述 GRE 的优缺点可以看出，GRE VPN 适合一些小型点对点的网络互联、实时性要求不高、要求提供地址空间重叠支持的网络环境。

9.5 本章小结

VPN 是将物理分布在不同地点的网络通过公用骨干网，尤其是 Internet 连接而成的逻辑上的虚拟子网。为了保障信息的安全，VPN 技术采用了鉴别、访问控制、保密性、完整性等措施，以防止信息被泄露、篡改和复制。

VPN 有 3 种类型：Access VPN、Intranet VPN 和 Extranet VPN。这 3 种类型的 VPN 分别对应于传统的远程访问网络、企业内部的 Intranet 以及企业和合作伙伴的网络所构成的 Extranet。

VPN 作为一种综合的网络安全方案，包含了很多重要的技术，最主要的是采用了密

码技术、身份认证技术、隧道技术和密钥管理技术 4 项技术。

第二层隧道协议有 L2F、PPTP 和 L2TP 等。L2F 已经过时，很少使用；PPTP 在微软的推动与支持下，已经成为一种事实上的工业标准，被广泛实现并已使用很长一段时间，目前大多数厂家均支持 PPTP；L2TP 作为下一代的隧道协议，是 PPTP 和 L2F 隧道功能的集合，其隧道并不局限于 TCP/IP，但是目前仅支持 IP。

GRE 协议提出较早，有很强的封装能力，不限于某个特定的“X over Y”应用，而是一种通用的封装形式。然而，GRE 协议既不进行加密，又不进行验证，因此通常与其他协议结合使用。

习　　题

1. 通常所说的移动 VPN 是指(　)。

   A. Access VPN　　B. Intranet VPN

   C. Extranet VPN　　D. 以上皆不是

2. 属于第二层的 VPN 隧道协议有(　)。

   A. IPSec　　B. PPTP　　C. GRE　　D. 以上皆不是

3. GRE 协议(　)。

   A. 既封装，又加密　　B. 只封装，不加密

   C. 不封装，只加密　　D. 不封装，不加密

4. PPTP 客户端使用(　)建立连接。

   A. TCP 协议　　B. UDP 协议　　C. L2TP 协议　　D. 以上皆不是

5. GRE 协议的乘客协议是(　)。

   A. IP　　B. IPX　　C. AppleTalk　　D. 上述皆可

6. VPN 分为几种类型？各种类型有何特点？

7. PPTP 和 L2TP 有何区别？

8. GRE 协议有何优缺点？

第10章 IPSec

本章要点：

- IPSec 的概念、功能、体系结构；
- 安全联盟和安全策略的概念；
- 传输模式和隧道模式的功能和特点；
- IPSec 安全协议的 AH 机制和功能；
- IPSec 安全协议的 ESP 机制和功能；
- 密钥管理协议 ISAKMP 机制和功能；
- Internet 的密钥交换协议 IKE 机制和功能。

10.1 IPSec 安全体系结构

10.1.1 IPSec 的概念

IPSec(IP Security)是一种由 IETF 设计的端到端的确保 IP 层通信安全的机制。IPSec 不是一个单独的协议，而是一组协议，这一点对于我们认识 IPSec 是很重要的。IPSec 协议的定义文件包括了12个 RFC 文件和几十个 Internet 草案，已经成为工业标准的网络安全协议。

IPSec 是随着 IPv6 的制定而产生的，鉴于 IPv4 的应用仍然很广泛，所以后来在 IPSec 的制定中也增加了对 IPv4 的支持。IPSec 在 IPv6 中是必须支持的，而在 IPv4 中是可选的。本章中提到 IP 协议时是指 IPv4 协议。

IP 协议在当初设计时并没有过多地考虑安全问题，而只是为了能够使网络方便地进行互联互通，因此 IP 协议从本质上就是不安全的。仅仅依靠 IP 头部的校验和字段无法保证 IP 包的安全，修改 IP 包并重新正确计算校验和是很容易的。如果不采取安全措施，IP 通信会暴露在多种威胁之下，下面举几个简单的例子。

(1) 窃听

一般情况下 IP 通信是明文形式的，第三方可以很容易地窃听到 IP 数据包并提取出其中的应用层数据。“窃听”虽然不破坏数据，却造成了通信内容外泄，甚至危及敏感数据的安全。

(2) 篡改

攻击者可以在通信线路上非法窃取到 IP 数据包，修改其内容并重新计算校验和，数据包的接收方一般不可能察觉出来。作为网络通信用户，即使并非所有的通信数据都是

高度机密的，也不想看到数据在传输过程中有任何差错。

(3) IP 欺骗

在一台机器上可以假冒另外一台机器向接收方发包。接收方无法判断收到的数据包是否真的来自该 IP 包中所声称的源 IP 地址。

(4) 重放攻击法

搜集特定的 IP 包，进行一定的处理，然后再一一重新发送，欺骗接收方主机。

IP 协议之所以如此不安全，就是因为 IP 协议没有采取任何安全措施，既没有对数据包的内容进行完整性验证，又没有进行加密。如今，IPSec 协议可以为 IP 网络通信提供透明的安全服务，保护 TCP/IP 通信免遭窃听和篡改，保证数据的完整性和机密性，有效抵御网络攻击，同时保持易用性。

表 10-1 列出了与 IPSec 相关的 RFC，如果想进一步了解 IPSec 的某些内容，请参考相关的网址 http://www.faqs.org/rfcs。

表 10-1 定义 IPSec 协议簇的各 RFC

RFC	内　　容
2401	IPSec 体系结构
2402	AH(Authentication Header)协议
2403	HMAC-MD5-96 在 AH 和 ESP 中的应用
2404	HMAC-SHA-1-96 在 AH 和 ESP 中的应用
2405	DES-CBC 在 ESP 中的应用
2406	ESP(Encapsulating Security Payload)协议
2407	IPSec DOI
2408	ISAKMP 协议
2409	IKE(Internet Key Exchange)协议
2410	NULL 加密算法及在 IPSec 中的应用
2411	IPSec 文档路线图
2412	OAKLEY 协议

10.1.2 IPSec 的功能

IPSec 具有以下功能：

(1) 作为一个隧道协议实现了 VPN 通信

IPSec 作为第三层的隧道协议，可以在 IP 层上创建一个安全的隧道，使两个异地的私有网络连接起来，或者使公网上的计算机可以访问远程的企业私有网络。这主要是通过隧道模式实现的，有关传输模式和隧道模式参见 10.1.6 小节。

(2) 保证数据来源可靠

在 IPSec 通信之前双方要先用 IKE 认证对方身份并协商密钥，只有 IKE 协商成功之后才能通信。由于第三方不可能知道验证和加密的算法以及相关密钥，因此无法冒充发

送方，即使冒充，也会被接收方检测出来。

(3) 保证数据完整性

IPSec 通过验证算法功能保证数据从发送方到接收方的传送过程中的任何数据篡改和丢失都可以被检测。

(4) 保证数据机密性

IPSec 通过加密算法使只有真正的接收方才能获取真正的发送内容，而他人无法获知数据的真正内容。

10.1.3　IPSec 体系结构

IPSec 众多的 RFC 通过如图 10-1 所示的关系图组织在一起。

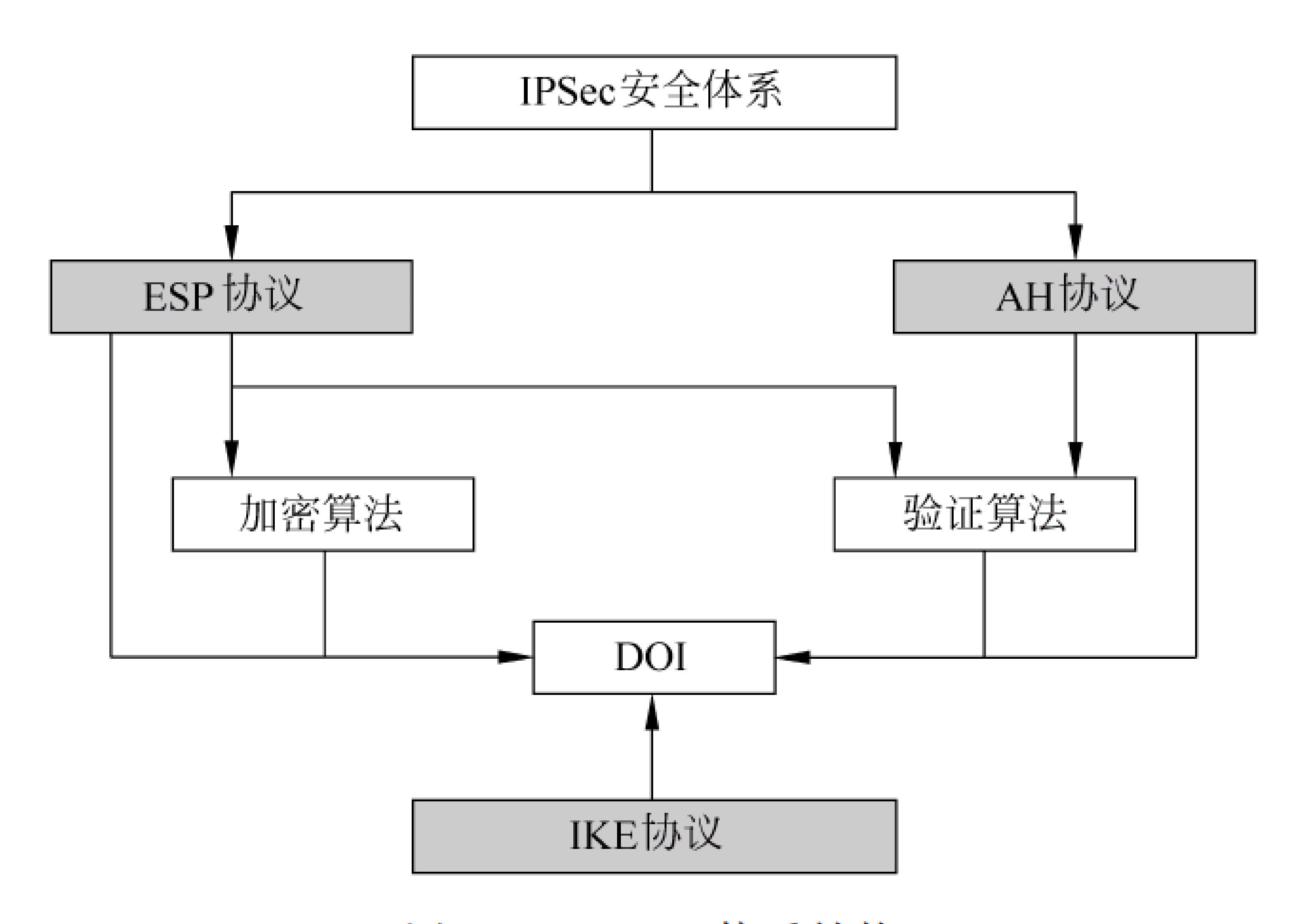


图 10-1　IPSec 体系结构

从图 10-1 中可以看出，IPSec 包含了 3 个最重要的协议：AH、ESP 和 IKE。

(1) AH 为 IP 数据包提供如下 3 种服务：无连接的数据完整性验证、数据源身份认证和防重放攻击。数据完整性验证通过哈希函数(如 MD5)产生的校验来保证；数据源身份认证通过在计算验证码时加入一个共享密钥来实现；AH 报头中的序列号可以防止重放攻击。

(2) ESP 除了为 IP 数据包提供 AH 已有的 3 种服务外，还提供另外两种服务：数据包加密、数据流加密。加密是 ESP 的基本功能，而数据源身份认证、数据完整性验证以及防重放攻击都是可选的。数据包加密是指对一个 IP 包进行加密，可以是对整个 IP 包，也可以只加密 IP 包的载荷部分，一般用于客户端计算机；数据流加密一般用于支持 IPSec 的路由器，源端路由器并不关心 IP 包的内容，对整个 IP 包进行加密后传输，目的端路由器将该包解密后将原始包继续转发。

AH 和 ESP 可以单独使用，也可以嵌套使用。通过这些组合方式，可以在两台主机、两台安全网关(防火墙和路由器)，或者主机与安全网关之间使用。

(3) IKE 协议负责密钥管理，定义了通信实体间进行身份认证、协商加密算法以及生成共享的会话密钥的方法。IKE 将密钥协商的结果保留在安全联盟(SA)中，供 AH 和

ESP 以后通信时使用。

最后，解释域(DOI)为使用 IKE 进行协商 SA 的协议统一分配标识符。共享一个 DOI 的协议从一个共同的命名空间中选择安全协议和变换、共享密码以及交换协议的标识符等，DOI 将 IPSec 的这些 RFC 文档联系到一起。

10.1.4　安全联盟和安全联盟数据库

1. 安全联盟(SA)

理解 SA 这一概念对于理解 IPSec 是至关重要的。AH 和 ESP 两个协议都使用 SA 来保护通信，而 IKE 的主要功能就是在通信双方协商 SA。

SA(Security Association，安全联盟)是两个 IPSec 实体(主机、安全网关)之间经过协商建立起来的一种协定，内容包括采用何种 IPSec 协议(AH 还是 ESP)、运行模式(传输模式还是隧道模式)、验证算法、加密算法、加密密钥、密钥生存期、抗重放窗口、计数器等，从而决定了保护什么、如何保护以及谁来保护。可以说 SA 是构成 IPSec 的基础。

SA 是单向的，进入(inbound)SA 负责处理接收到的数据包，外出(outbound)SA 负责处理要发送的数据包。因此每个通信方必须要有两种 SA，一个进入 SA，一个外出 SA，这两个 SA 构成了一个 SA 束(SA Bundle)。

SA 的管理包括创建和删除，有以下两种管理方式。

(1) 手工管理：SA 的内容由管理员手工指定、手工维护。但是，手工维护容易出错，而且手工建立的 SA 没有生存周期限制，一旦建立了，就不会过期，除非手工删除，因此有安全隐患。

(2) IKE 自动管理：一般来说，SA 的自动建立和动态维护是通过 IKE 进行的。利用 IKE 创建和删除 SA，不需要管理员手工维护，而且 SA 有生命期。如果安全策略要求建立安全、保密的连接，但又不存在与该连接相应的 SA，IPSec 的内核会立刻启动 IKE 来协商 SA。

每个 SA 由三元组〈SPI，源/目的 IP 地址，IPSec 协议〉唯一标识，这 3 项含义如下：

- SPI(Security Parameter Index，安全参数索引)是 32 位的安全参数索引，标识同一个目的地的 SA。
- 源/目的 IP 地址：表示对方 IP 地址，对于外出数据包，指目的 IP 地址；对于进入 IP 包，指源 IP 地址。
- IPSec 协议：采用 AH 或 ESP。

2. 安全联盟数据库(SAD)

SAD(Security Association Database，安全联盟数据库)并不是通常意义上的“数据库”，而是将所有的 SA 以某种数据结构集中存储的一个列表。对于外出的流量，如果需要使用 IPSec 处理，然而相应的 SA 不存在，则 IPSec 将启动 IKE 来协商出一个 SA，并存储到 SAD 中。对于进入的流量，如果需要进行 IPSec 处理，IPSec 将从 IP 包中得到三元组，并利用这个三元组在 SAD 中查找一个 SA。

SAD 中每一个 SA 除了上面的三元组之外，还包括下面这些内容。

(1) 本方序号计数器:32 位,用于产生 AH 或 ESP 头的序号字段,仅用于外出数据包。SA 刚建立时,该字段值设置为 0,每次用 SA 保护完一个数据包时,就把序列号的值递增 1,对方利用这个字段来检测重放攻击。通常在这个字段溢出之前,SA 会重新进行协商。

(2) 对方序号溢出标志:标识序号计数器是否溢出。如果溢出,则产生一个审计事件,并禁止用 SA 继续发送数据包。

(3) 抗重放窗口:32 位计数器,用于决定进入的 AH 或 ESP 数据包是否为重发的。仅用于进入数据包,如接收方不选择抗重放服务(如手工设置 SA 时),则不用抗重放窗口。

(4) AH 验证算法、密钥等。

(5) ESP 加密算法、密钥、IV(Initial Vector)模式、IV 等。如不选择加密,该字段为空。

(6) ESP 验证算法、密钥等。如不选择验证,该字段为空。

(7) SA 的生存期:表示 SA 能够存在的最长时间。生存期的衡量可以用时间也可以用传输的字节数,或将两者同时使用,优先采用先到期者。SA 过期之后应建立一个新的 SA 或终止通信。

(8) 运行模式:是传输模式还是隧道模式。

(9) PMTU:所考察的路径的 MTU 及其 TTL 变量。

10.1.5　安全策略和安全策略数据库

SP(Security Policy,安全策略)指示对 IP 数据包提供何种保护,并以何种方式实施保护。SP 主要根据源 IP 地址、目的 IP 地址、入数据还是出数据等来标识。IPSec 还定义了用户能以何种粒度来设定自己的安全策略,由“选择符”来控制粒度的大小,不仅可以控制到 IP 地址,还可以控制到传输层协议或者 TCP/UDP 端口等。

SPD(Security Policy Database,安全策略数据库)也不是通常意义上的“数据库”,而是将所有的 SP 以某种数据结构集中存储的列表。

当要将 IP 包发送出去时,或者接收到 IP 包时,首先要查找 SPD 来决定如何进行处理。存在 3 种可能的处理方式:丢弃、不用 IPSec 和使用 IPSec。

(1) 丢弃:流量不能离开主机或者发送到应用程序,也不能进行转发。

(2) 不用 IPSec:对流量作为普通流量处理,不需要额外的 IPSec 保护。

(3) 使用 IPSec:对流量应用 IPSec 保护,此时这条安全策略要指向一个 SA。对于外出流量,如果该 SA 尚不存在,则启动 IKE 进行协商,把协商的结果连接到该安全策略上。

10.1.6　IPSec 运行模式

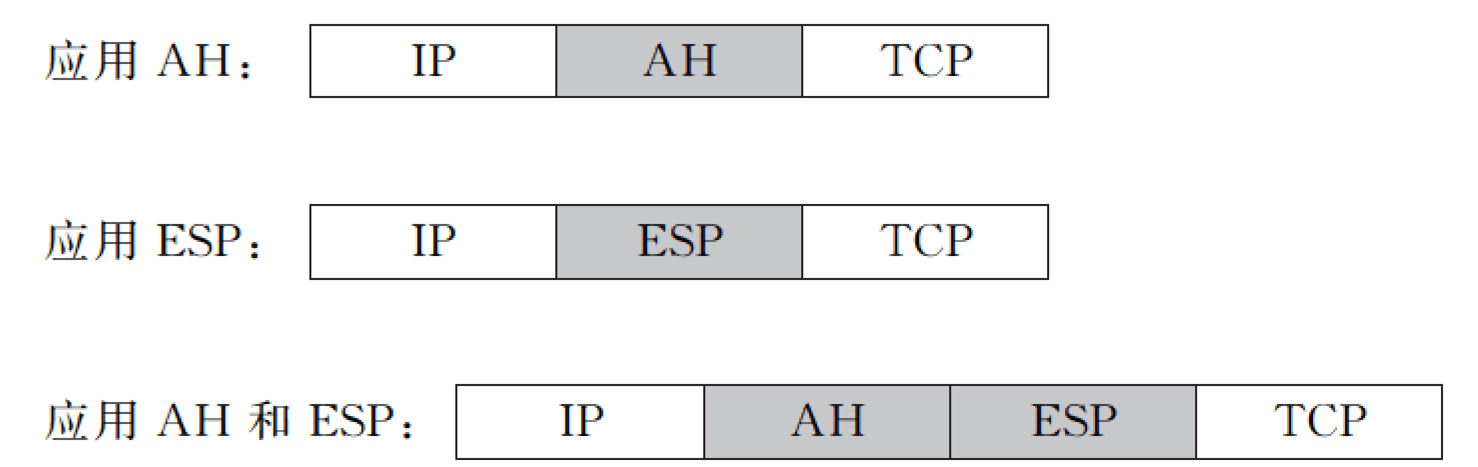
IPSec 有两种运行模式:传输模式(Transport Mode)和隧道模式(Tunnel Mode)。AH 和 ESP 都支持这两种模式,因此有 4 种可能的组合:传输模式的 AH、隧道模式的 AH、传输模式的 ESP 和隧道模式的 ESP。

1. IPSec 传输模式

传输模式要保护的内容是 IP 包的载荷，可能是 TCP/UDP 等传输层协议，也可能是 ICMP 协议，还可能是 AH 或者 ESP 协议（在嵌套的情况下）。传输模式为上层协议提供安全保护。通常情况下，传输模式只用于两台主机之间的安全通信。

正常情况下，传输层数据包在 IP 中被添加一个 IP 头部构成 IP 包。启用 IPSec 之后，IPSec 会在传输层数据前面增加 AH 或者 ESP 或者两者同时增加，构成一个 AH 数据包或者 ESP 数据包，然后再添加 IP 头部组成新的 IP 包。

以 TCP 协议为例，应用 IPSec 之后包的格式有下面 3 种可能（阴影表示新增的部分）。



2. IPSec 隧道模式

隧道模式保护的内容是整个原始 IP 包，隧道模式为 IP 协议提供安全保护。通常情况下，只要 IPSec 双方有一方是安全网关或路由器，就必须使用隧道模式。

如果路由器要为自己转发的数据包提供 IPSec 安全服务，就要使用隧道模式。路由器主要依靠检查 IP 头部来做出路由决定，不会也不应该修改 IP 头部以外的其他内容。如果路由器对要转发的包插入传送模式的 AH 或 ESP 头部，便违反了路由器的规则。

路由器将需要进行 IPSec 保护的原始 IP 包看作一个整体，将这个 IP 包作为要保护的内容，前面添加 AH 或者 ESP 头部，然后再添加新的 IP 头部，组成新的 IP 包之后再转发出去。以 ESP 为例，示意如下。

应用 ESP：

IP	ESP	IP+TCP

IPSec 隧道模式的数据包有两个 IP 头：内部头和外部头。内部头由路由器背后的主机创建，外部头由提供 IPSec 的设备（可能是主机，也可能是路由器）创建。隧道模式下，通信终点由受保护的内部 IP 头指定，而 IPSec 终点则由外部 IP 头指定。如 IPSec 终点为安全网关，则该网关会还原出内部 IP 包，再转发到最终目的地。

10.2　IPSec 安全协议——AH

10.2.1　AH 概述

AH（Authentication Header，验证头部协议）由 RFC2402 定义，是用于增强 IP 层安

全的一个 IPSec 协议，该协议可以提供无连接的数据完整性、数据来源验证和抗重放攻击服务。

AH 协议对 IP 层的数据使用密码学中的验证算法，从而使得对 IP 包的修改可以被检测出来。具体地说，这个验证算法是密码学中的 MAC（Message Authentication Codes，报文验证码）算法，MAC 算法将一段给定的任意长度的报文和一个密钥作为输入，产生一个固定长度的输出报文，称为报文摘要或者指纹。MAC 算法与 HASH 算法非常相似，区别在于 MAC 算法需要一个密钥（key），而 HASH 算法不需要。实际上，MAC 算法一般是由 HASH 算法演变而来，也就是将输入报文和密钥结合在一起然后应用 HASH 算法。这种 MAC 算法称为 HMAC，例如 HMAC-MD5、HMAC-SHA1、HMAC-RIPEMD-160。

通过 HMAC 算法可以检测出对 IP 包的任何修改，不仅包括对 IP 包的源/目的 IP 地址的修改，还包括对 IP 包载荷的修改，从而保证了 IP 包内容的完整性和 IP 包来源的可靠性。为了使通信双方能产生相同的报文摘要，通信双方必须采用相同的 HMAC 算法和密钥。对同一段报文使用不同的密钥来产生相同的报文摘要是不可能的。因此，只有采用相同的 HMAC 算法并共享密钥的通信双方才能产生相同的验证数据。

不同的 IPSec 系统，其可用的 HMAC 算法也可能不同，但是有两个算法是所有 IPSec 都必须实现的：HMAC-MD5 和 HMAC-SHA1。

10.2.2　AH 头部格式

AH 协议和 TCP、UDP 协议一样，是被 IP 协议封装的协议之一。一个 IP 包的载荷是否是 AH 协议，由 IP 协议头部中的协议字段判断，正如 TCP 协议是 6，UDP 协议是 17 一样，AH 协议是 51。如果一个 IP 包封装的是 AH 协议，在 IP 包头（包括选项字段）后面紧跟的就是 AH 协议头部，格式如图 10-2 所示。AH 头部格式包括以下内容。

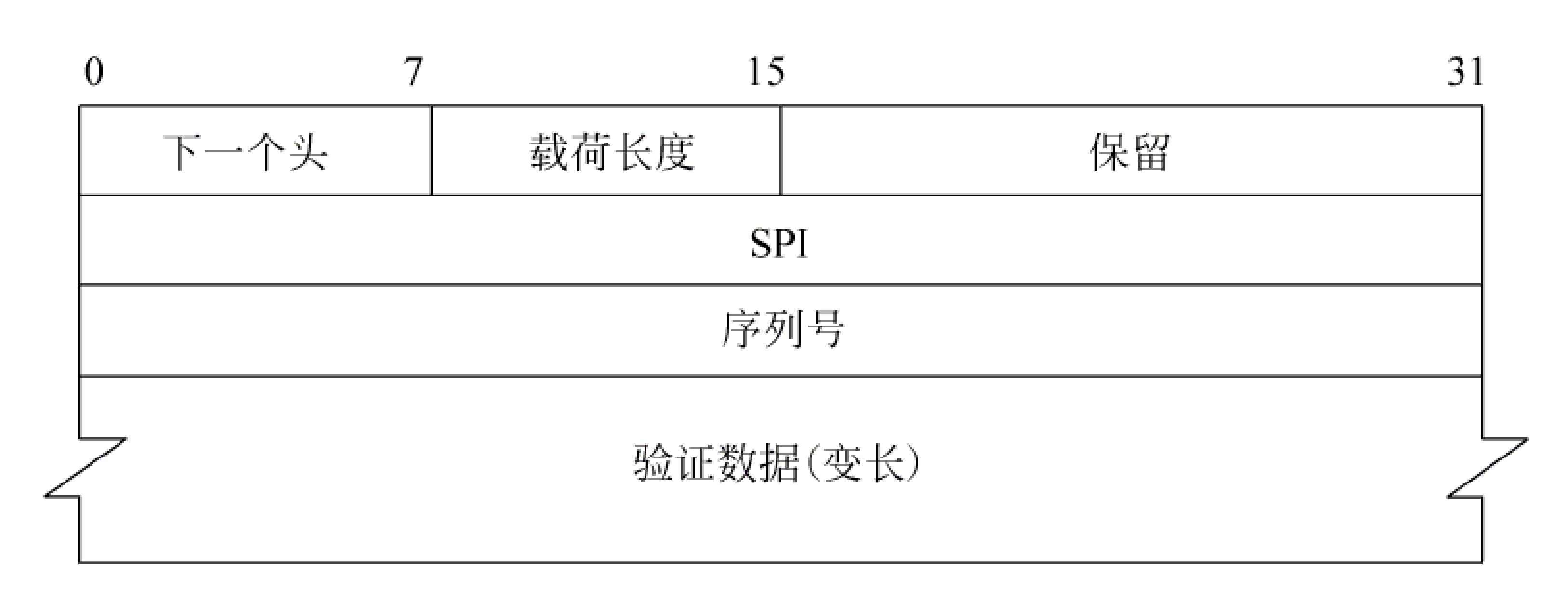


图 10-2　AH 头部

（1）下一个头（Next Header）

最开始的 8 位，表示紧跟在 AH 头部的下一个载荷的类型，也就是紧跟在 AH 头部后面数据的协议。在传输模式下，该字段是处于保护中的传输层协议的值，比如6（TCP）、17（UDP）或者 50（ESP）。在隧道模式下，AH 所保护的是整个 IP 包，该值是 4，表示 IP-in-IP 协议。

（2）载荷长度（Payload Length）

接下来的 8 位，其值是以 32 位（4 字节）为单位的整个 AH 数据（包括头部和变长的

认证数据)的长度再减 2。

(3) 保留(reserved)

16 位,作为保留用,实现中应全部设置为 0。

(4) SPI(Security Parameter Index,安全参数索引)

SPI 是一个 32 位整数,与源/目的 IP 地址、IPSec 协议一起组成的三元组可以为该 IP 包唯一地确定一个 SA。[1,255]保留为将来使用,0 保留本地的特定实现使用。因此,可用的 SPI 值为[256,$2^{32}-1$]。

(5) 序列号(Sequence Number)

序列号是一个 32 位整数,作为一个单调递增的计数器,为每个 AH 包赋予一个序号。当通信双方建立 SA 时,计数器初始化为 0。SA 是单向的,每发送一个包,外出 SA 的计数器增 1;每接收一个包,进入 SA 的计数器增 1。该字段可以用于抵抗重放攻击。

(6) 验证数据(Authentication Data)

可变长部分,包含了验证数据,也就是 HMAC 算法的结果,称为 ICV(Integrity Check Value,完整性校验值)。该字段必须为 32 位的整数倍,如果 ICV 不是 32 位的整数倍,必须进行填充,用于生成 ICV 的算法由 SA 指定。

10.2.3　AH运行模式

AH 有两种运行模式:传输模式和隧道模式。

1. AH传输模式

在传输模式中,AH 插入到 IP 头部(包括 IP 选项字段)之后,传输层协议(如 TCP、UDP)或者其他 IPSec 协议之前。以 TCP 数据为例,图 10-3 表示了 AH 在传输模式中的位置。

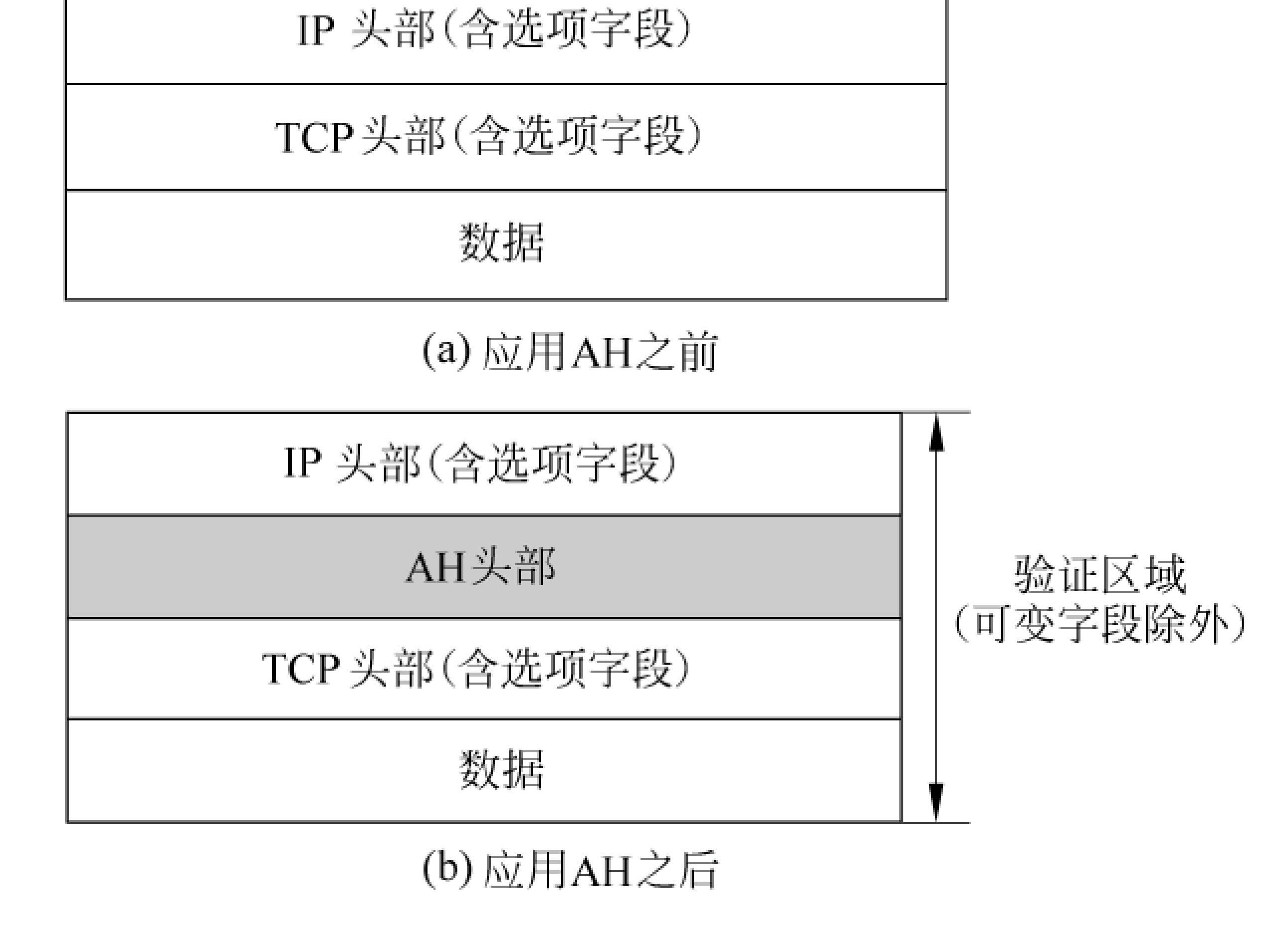


图 10-3　AH 传输模式

从图 10-3 可以看出,被 AH 验证的区域是整个 IP 包(可变字段除外,有关可变字段

参见 10.2.4 小节），包括 IP 包头部，因此源 IP 地址、目的 IP 地址是不能修改的，否则会被检测出来。然而，如果该包在传送的过程中经过 NAT（Network Address Translation，网络地址转换）网关，其源/目的 IP 地址将被改变，将造成到达目的地址后的完整性验证失败。因此，AH 在传输模式下和 NAT 是冲突的，不能同时使用，或者可以说 AH 不能穿越 NAT。

2. AH隧道模式

在隧道模式中，AH 插入到原始 IP 头部字段之前，然后在 AH 之前再增加一个新的 IP 头部。以 TCP 为例，图 10-4 表示了 AH 在隧道模式中的位置。

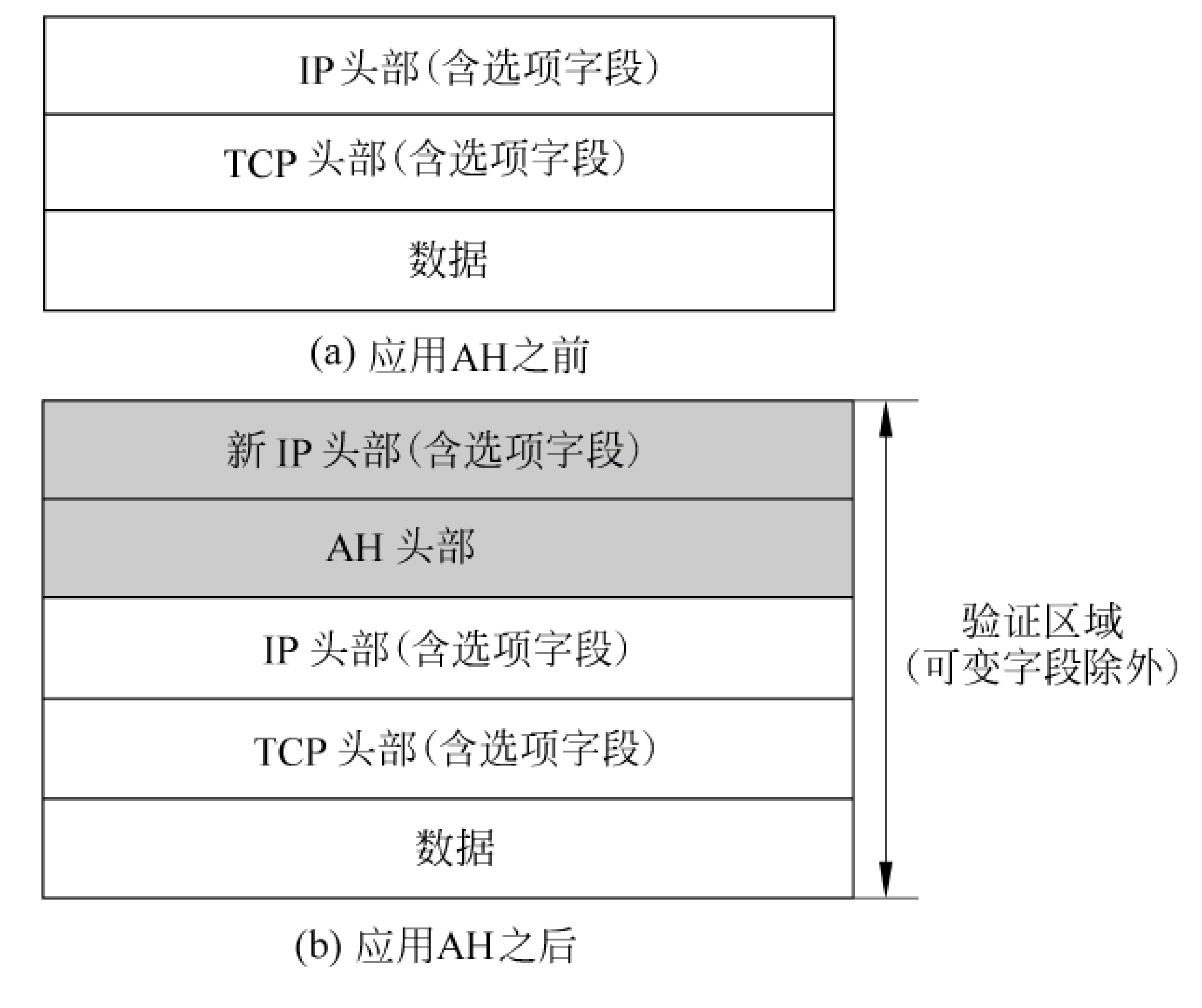


图 10-4　AH 隧道模式

隧道模式下，AH 验证的范围也是整个 IP 包，因此上面讨论的 AH 和 NAT 的冲突在隧道模式下也存在。

在隧道模式中，AH 可以单独使用，也可以和 ESP 一起嵌套使用。

10.2.4　数据完整性检查

在应用 AH 进行处理时，相应的 SA 应该已经建立，因此 AH 所用到的 HMAC 算法和密钥已经确定。从上面的传输模式和隧道模式可以看出，AH 协议验证的范围包括整个 IP 包，验证过程概括如下：在发送方，整个 IP 包和验证密钥被作为输入，经过 HMAC 算法计算后得到的结果被填充到 AH 头部的“验证数据”字段中；在接收方，整个 IP 包和验证算法所用的密钥也被作为输入，经过 HMAC 算法计算的结果和 AH 头部的“验证数据”字段进行比较，如果一致，说明该 IP 包数据没有被篡改，内容是真实可信的。

在应用 HMAC 算法时，有一些因素需要考虑。在 IP 字段中，有一些是可变的，而且在传输过程中被修改也是合理的，不能说明该数据包是被非法篡改的。这些字段在计算 HMAC 时被临时用 0 填充，具体包括如下。

- ToS（Type of Service）：8 位的服务类型字段指出了延时、吞吐量和可靠性方面的

要求。某些路由器会修改该字段以达到特定的 QoS 服务质量。
- 标志字段：这是指用于表示分片的 3 位标志——DF（Don't Fragment）、MF（More Fragments）和 0。路由器可能会修改这 3 个标志。
- 分片偏移字段：标志字段后面的 13 位的偏移字段。
- TTL：生命期，为了防止 IP 包的无限次路由，每经过一个路由器，该字段减 1，当 TTL 变为 0 时，被路由器抛弃。
- 头部校验和：中间路由器对 IP 包头部作了任何修改之后，必须重新计算头部校验和，因此该字段也是可变的。
- 选项字段。

另外，AH 头部的验证数据字段在计算之前也要用 0 填充，计算之后再填充验证结果。

对于一个 IP 包，除上述可变字段外，其余部分都认为是应该不变的，这些部分也正是受到 AH 协议保护的部分。具体来说，这些不变的部分包括如下。
- 版本字段。
- 头部长度字段。
- IP 总长字段。
- ID 字段。
- 协议字段。
- 源 IP 地址字段。
- 目的地址字段。
- AH 头中除"验证数据"以外的其他字段。
- 数据：指经过 AH 处理之后，在 AH 头部后面的数据。传输方式下，指 TCP、UDP 或 ICMP 等传输层数据；隧道模式下，指被封装的原 IP 包。

10.3 IPSec 安全协议——ESP

10.3.1 ESP 概述

与 AH 一样，ESP（Encapsulating Security Payload，封装安全载荷）协议也是一种增强 IP 层安全的 IPSec 协议，由 RFC2406 定义。ESP 协议除了可以提供无连接的完整性、数据来源验证和抗重放攻击服务之外，还提供数据包加密和数据流加密服务。

ESP 协议提供数据完整性和数据来源验证的原理和 AH 一样，也是通过验证算法实现。然而，与 AH 相比，ESP 验证的数据范围要小一些。ESP 协议规定了所有 IPSec 系统必须实现的验证算法：HMAC-MD5、HMAC-SHA1、NULL。NULL 认证算法是指实际不进行认证。

数据包加密服务通过对单个 IP 包或 IP 包载荷应用加密算法实现；数据流加密是通过隧道模式下对整个 IP 包应用加密算法实现。ESP 的加密采用的是对称密钥加密算法。

与公钥加密算法相比，对称加密算法可以提供更大的加密/解密吞吐量。不同的 IPSec 实现，其加密算法也有所不同。为了保证互操作性，ESP 协议规定了所有 IPSec 系统都必须实现的算法：DES-CBC、NULL。NULL 加密算法是指实际不进行加密。

之所以有 NULL 算法，是因为加密和认证都是可选的，但是 ESP 协议规定加密和认证不能同时为 NULL。换句话说，如果采用 ESP，加密和认证至少必选其一，当然也可以两者都选，但是不能两者都不选。

10.3.2　ESP 头部格式

ESP 协议和 TCP、UDP、AH 协议一样，是被 IP 协议封装的协议之一。一个 IP 包的载荷是否是 ESP 协议，由 IP 协议头部中的协议字段判断，ESP 协议字段是 50。如果一个 IP 包封装的是 ESP 协议，在 IP 包头（包括选项字段）后面紧跟的就是 ESP 协议头部，格式如图 10-5 所示。ESP 头部格式包括以下内容。

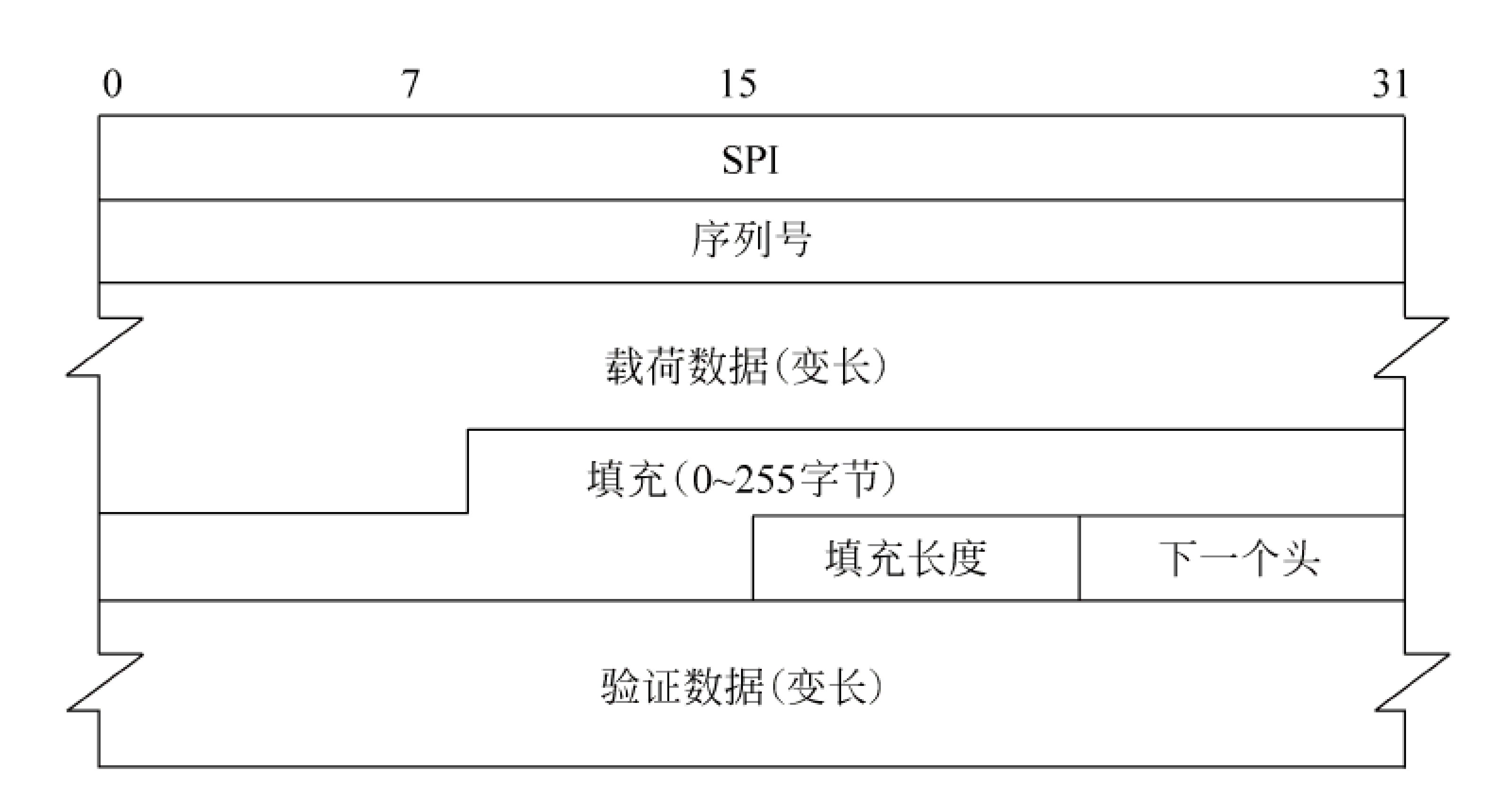


图 10-5　ESP 头部格式

（1）SPI

SPI 是一个 32 位整数，与源/目的 IP 地址、IPSec 协议一起组成的三元组可以为该 IP 包唯一地确定一个 SA。

（2）序列号（Sequence Number）

序列号是一个 32 位整数，作为一个单调递增的计数器，为每个 ESP 包赋予一个序号。当通信双方建立 SA 时，计数器初始化为 0。SA 是单向的，每发送一个包，外出 SA 的计数器增 1；每接收一个包，进入 SA 的计数器增 1。该字段可以用于抵抗重放攻击。

（3）载荷数据（Payload Data）

这是变长字段，包含了实际的载荷数据。不管 SA 是否需要加密，该字段总是必需的。如果采用了加密，该部分就是加密后的密文；如果没有加密，该部分就是明文。如果采用的加密算法需要一个 IV（Initial Vector，初始向量），IV 也是在本字段中传输的。该加密算法的规范必须能够指明 IV 的长度以及在本字段中的位置。本字段的长度必须是 8 位的整数倍。

(4) 填充(Padding)

填充字段包含了填充位。

(5) 填充长度(Pad Length)

填充长度字段是一个 8 位字段,以字节为单位指示了填充字段的长度,其范围为[0,255]。

(6) 下一个头(Next Header)

8 位字段,指明了封装在载荷中的数据类型,例如 6 表示 TCP 数据。

(7) 验证数据(Authentication Data)

变长字段。只有选择了验证服务时才会有该字段,包含了验证的结果。

10.3.3　ESP 运行模式

和 AH 一样,ESP 也有两种运行模式:传输模式和隧道模式。运行模式决定了 ESP 插入的位置以及保护的对象。

1. ESP 传输模式

传输模式保护的是 IP 包的载荷,例如 TCP、UDP、ICMP 等,也可以是其他 IPSec 协议的头部。ESP 插入到 IP 头部(含选项字段)之后,任何被 IP 协议所封装的协议(如传输层协议 TCP、UDP、ICMP,或者 IPSec 协议)之前。以 TCP 为例,图 10-6 是在应用 ESP 传输模式前后的 IP 包格式。



(a) 应用ESP之前



(b) 应用ESP之后

图 10-6　ESP 传输模式

在图 10-6 中,ESP 头部包含 SPI 和序号字段,ESP 尾部包含填充、填充长度和下一个头字段。被加密和被验证的区域在图中已经表示出来了。

如果使用了加密,SPI 和序号字段不能被加密。首先,在接收端,SPI 字段用于和源 IP 地址、IPSec 协议一起组成一个三元组来唯一确定一个 SA,利用该 SA 进行验证、解密等后续处理。如果 SPI 被加密了,要解密之就必须找到 SA,而查找 SA 又需要 SPI,这样

就产生了类似于“先有鸡还是先有鸡蛋”的问题。因此，SPI 不能被加密。其次，序号字段用于判断包是否重复，从而可以防止重放攻击。序号字段不会泄露明文中的任何机密，没有必要进行加密。不加密序号字段也使得一个包不经过烦琐的解密过程就可以判断包是否重复，如果重复则丢弃之，节省了时间和资源。

如果使用了验证，验证数据也不会被加密，因为如果 SA 需要 ESP 的验证服务，那么接收端会在进行任何后续处理(如检查重放、解密)之前进行验证。数据包只有经过验证证明该包没有经过任何修改，是可以信任的，才会进行后续处理。

值得注意的是，和 AH 不同，ESP 的验证不会对整个 IP 包进行验证，IP 包头部(含选项字段)不会被验证。因此，ESP 不存在像 AH 那样的和 NAT 模式冲突的问题。如果通信的任何一方具有私有地址或者在安全网关背后，双方的通信仍然可以用 ESP 来保护其安全，因为 IP 头部中的源/目的 IP 地址和其他字段不被验证，可以被 NAT 网关或者安全网关修改。

当然，ESP 在验证上的这种灵活性也有缺点：除了 ESP 头部之外，任何 IP 头部字段都可以修改，只要保证其校验和计算正确，接收端就不能检测出这种修改。所以，ESP 传输模式的验证服务要比 AH 传输模式弱一些。如果需要更强的验证服务并且通信双方都是公有 IP 地址，应该采用 AH 来验证，或者将 AH 认证与 ESP 验证同时使用。

2 ESP 隧道模式

隧道模式保护的是整个 IP 包，对整个 IP 包进行加密。ESP 插入到原 IP 头部(含选项字段)之前，在 ESP 之前再插入新的 IP 头部。以 TCP 为例，图 10-7 是在应用 ESP 传输模式前后的 IP 包格式。

在隧道模式下，有两个 IP 头部。里面的 IP 头部是原始的 IP 头部，含有真实的源 IP 地址、最终的目的 IP 地址；外面的 IP 头部可以包含与里面 IP 头部不同的 IP 地址，例如，可以是 NAT 网关的 IP 地址，这样两个子网中的主机可以利用 ESP 进行安全通信。

与传输模式一样，ESP 头部含有 SPI 和序号字段；ESP 尾部含有填充、填充头部和下一个头字段；如果选用了验证，ESP 的验证数据字段中包含了验证数据。同样，ESP 头部和 ESP 验证数据字段不被加密。

隧道模式中的加密和验证的范围如图 10-7 所示，内部 IP 头部被加密和验证，而外部 IP 头部既不被加密也不被验证。不被加密是因为路由器需要这些信息来为其寻找路由；不被验证是为了能适用于 NAT 等情况。

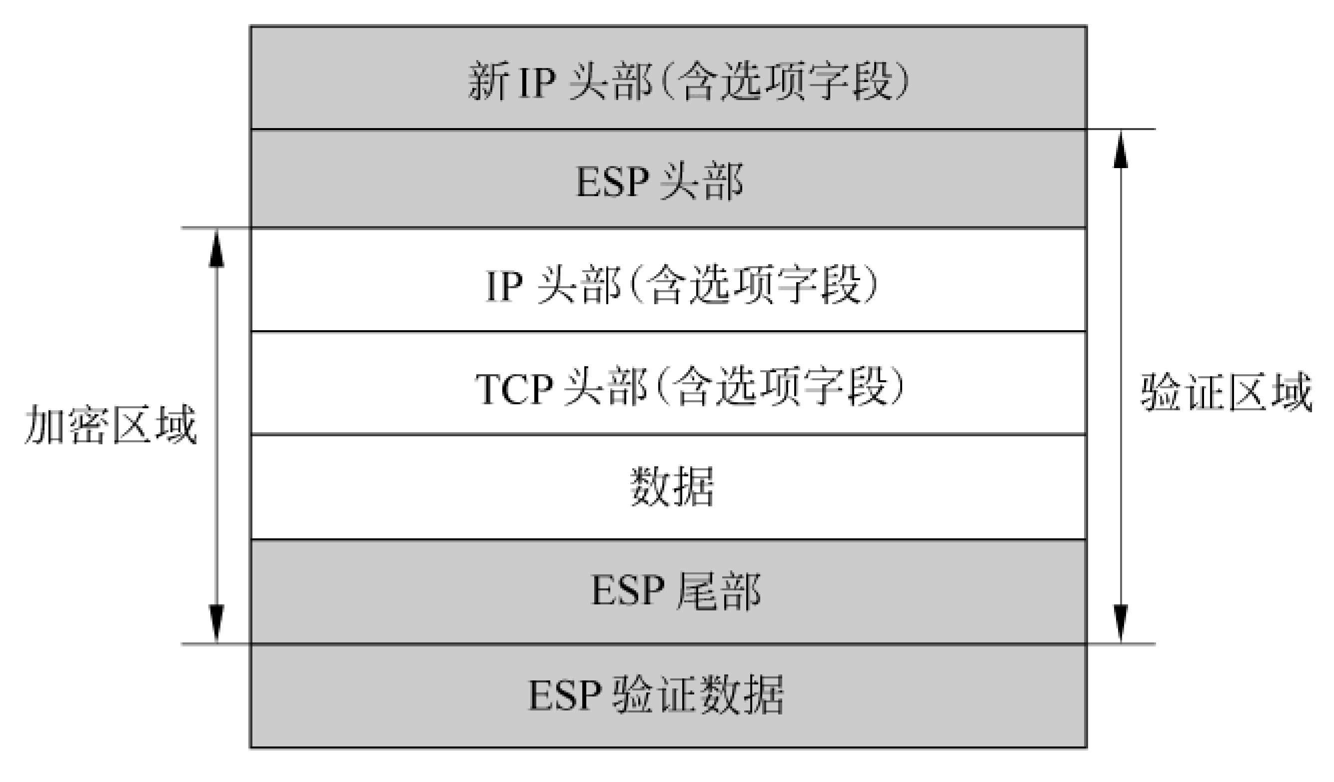
重要的是，ESP 隧道模式的验证和加密能够提供比 ESP 传输模式更加强大的安全功能，因为隧道模式下对整个原始 IP 包进行验证和加密，可以提供数据流加密服务；而 ESP 在传输模式下不能提供流加密服务，因为源、目的 IP 地址不被加密。

不过，隧道模式下将占用更多的带宽，因为隧道模式要增加一个额外的 IP 头部。因此，如果带宽利用率是一个关键问题，则传输模式更合适。

尽管 ESP 隧道模式的验证功能不像 AH 传输模式或隧道模式那么强大，但 ESP 隧道模式提供的安全功能已经足够了。



(a) 应用ESP之前



(b) 应用ESP之后

图 10-7　ESP 隧道模式

10.4　ISAKMP 协议

10.4.1　ISAKMP 概述

ISAKMP(Internet Security Association Key Management Protocol,Internet 安全联盟密钥管理协议)由 RFC2408 定义,定义了协商、建立、修改和删除 SA 的过程和包格式。ISAKMP 只是为 SA 的属性和协商、修改、删除 SA 的方法提供了一个通用的框架,并没有定义具体的 SA 格式。ISAKMP 没有定义任何密钥交换协议的细节,也没有定义任何具体的加密算法、密钥生成技术或者认证机制。这个通用的框架是与密钥交换独立的,可以被不同的密钥交换协议使用。

ISAKMP 报文可以利用 UDP 或者 TCP,端口都是 500,一般情况下常用 UDP 协议。

ISAKMP 双方交换的内容称为载荷(payload),ISAKMP 目前定义了 13 种载荷,一个载荷就像积木中的一个"小方块",这些载荷按照某种规则"叠放"在一起,然后在最前面添加上 ISAKMP 头部,这样就组成了一个 ISAKMP 报文,这些报文按照一定的模式进行交换,从而完成 SA 的协商、修改和删除等功能。

在讨论具体载荷之前,先看看 ISAKMP 载荷头部格式。

10.4.2　ISAKMP 包头部格式

ISAKMP 报文的头部是固定长度的,包含了维护状态、处理载荷必要的信息;头部后

面的载荷数目不定。ISAKMP 报文头部格式如图 10-8 所示。ISAKMP 报文头部格式包括以下内容。



图 10-8 ISAKMP 报文头部

(1) 发起方 Cookie(Initiator Cookie)

发起方的 Cookie，长度为 64 位(8 字节)。Cookie 可以帮助通信双方确认一个 ISAKMP 报文是否真的来自对方。在发起方，如果收到的某报文的应答方 Cookie 字段和以前收到的该字段不同，则丢弃该报文；同样，在应答方，如果收到的某报文的发起方 Cookie 和以前收到的该字段不同，则丢弃该报文。这种机制可以防止 DOS 攻击。

尽管 Cookie 的生成方法在实现不同的 ISAKMP 时可能不同，但无论发起方还是响应方，Cookie 必须满足两个条件：①Cookie 必须是用各自的机密信息生成的，该机密信息不能从 Cookie 中推导出来；②对于一个 SA，其 Cookie 是唯一的，也就是说对于一次 SA 协商过程，Cookie 不能改变。

常用的一个生成 Cookie 的方法是对下述信息进行 HASH(MD5、SHA1 或其他 HASH 算法)之后，取结果的前 64 位：

源 IP 地址＋目的 IP 地址＋UDP 源端口＋UDP 目的端口＋随机数＋当前日期＋当前时间

(2) 应答方 Cookie(Responder Cookie)

应答方的 Cookie，紧跟在发起方 Cookie 之后，长度为 64 位(8 字节)。

(3) 下一个载荷(Next Payload)

表示紧跟在 ISAKMP 头部之后的第一个载荷的类型值。目前定义了 13 种载荷，类型值如表 10-2 所示。

表 10-2 ISAKMP 定义的载荷类型值

载 荷 类 型	值
None	0
SA 载荷(Security Association)	1
建议载荷(proposal)	2
变换载荷(transform)	3
密钥交换载荷(Key Exchange)	4
身份载荷(identification)	5

续表

载荷类型	值
证书载荷(certificate)	6
证书请求载荷(Certificate Request)	7
HASH 载荷(Hash)	8
签名载荷(signature)	9
NONCE 载荷(nonce)	10
通知载荷(notification)	11
删除载荷(delete)	12
厂商载荷(vendor)	13
保留	14～127
私有用途	128～255

(4) 主版本(Major Version)

长度为 4 位,表示 ISAKMP 协议的主版本号。

(5) 次版本(Minor Version)

长度为 4 位,表示 ISAKMP 协议的次版本号。

(6) 交换类型(Exchange Type)

长度为 8 位,表示该报文所属的交换类型。目前定义了 5 种交换类型,如表 10-3 所示。

(7) 标志(Flags)

长度为 8 位,目前只有后 3 位有用,其余保留,用 0 填充。后 3 位的含义从最后一位往前依次为:

- 加密位(encryption),0x01。加密位如果是 1,表示 ISAKMP 头部后面的所有载荷都被加密了;如果是 0,表示载荷是明文,没有加密。
- 提交位(commit),0x02。
- 纯验证位(Authentication Only),0x04。

表 10-3 ISAKMP 交换类型

交换类型	值
None	0
基本交换(base)	1
身份包含交换(Identity Protection)	2
纯认证交换(Authentication Only)	3
积极交换(aggressive)	4
信息交换(informational)	5
ISAKMP 将来使用	6～31
DOI 专用	32～239
私有用途	240～255

(8) 报文 ID(Message ID)

长度 32 位,包含的是由第二阶段协商的发起方生成的随机值,这个唯一的报文标识可以唯一确定第二阶段的协议状态。

(9) 报文长度(length)

长度 32 位,以字节为单位表示了 ISAKMP 整个报文(头部 + 若干载荷)的总长度。

10.4.3　ISAKMP 载荷头部

不论何种载荷,都有一个相同格式的载荷头部,图 10-9 表示了这个通用的载荷头部格式。载荷头部格式包括以下内容。

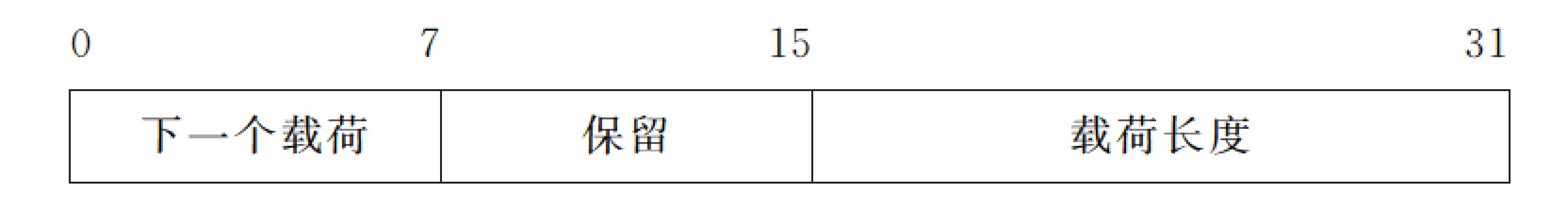


图 10-9　载荷头部

(1) 下一个载荷(Next Payload)

8 位字段,表示紧跟在本载荷后面的下一个载荷的类型。通过该字段,不同的载荷可以像链条一样链接起来,每个载荷的类型都在前一个载荷中指明,第一个载荷的类型在 ISAKMP 头部中指明,最后一个载荷的 Next Payload 类型为 0,从而指明这是最后一个载荷。

(2) 保留(reserved)

保留用,8 位字段,全 0。

(3) 载荷长度(Payload Length)

以字节为单位表示的载荷长度(包括载荷头部),16 位字段,该字段定义了每个载荷的边界。

10.4.4　ISAKMP 载荷

1. SA 载荷

SA 载荷用于协商 SA,并且指出协商发生的环境,也就是 DOI。ISAKMP 协议只是为协商、修改、删除 SA 的过程定义了一个框架,而 SA 的内容、SA 的属性、某些载荷的特定字段等还需要应用 ISAKMP 的协议来具体定义和实现,这些具体的实现就构成了 DOI,比如正在讨论的 IPSec 就是一种 DOI。

2. 建议载荷(proposal)

建议载荷包含的是在 SA 协商过程中用到的信息。该载荷提供了一个框架,利用这个框架发起方向接收方发送自己的建议,例如期望的 IPSec 协议和其他安全机制。

3. 变换载荷(transform)

变换载荷包括变换编号(Transform Number)和变换 ID(Transform ID);前者表示本载荷在建议载荷中的编号,后者确定变换 ID 取值。

4. 密钥交换载荷(Key Exchange)

密钥交换载荷用于传输密钥交换数据,这个载荷不局限于任何密钥交换协议。除了通用载荷头部外,该载荷只包含一个变长的密钥交换数据字段,该字段的组成格式及如何解释由具体的密钥交换协议具体定义,因此,该载荷适用于任何通常用的密钥交换协议。

5. 身份载荷(identification)

通信双方利用身份载荷互相交换身份信息。在 SA 协商的时候,发起方要通过该载荷告诉对方自己的身份,而响应方利用发起方的身份来决定应该采用何种安全策略。

6. 证书载荷(certificate)

证书载荷允许通信双方交换各自的证书,或者与证书相关的其他内容。

7. 证书请求载荷(Certificate Request)

通信双方可以利用证书请求载荷来请求对方发送证书。一方在收到该请求后,如果支持证书,就必须利用证书载荷来发送对方所请求的证书。如果有多个证书,请求方就必须发送多次证书请求载荷,接收方发送多次证书载荷。

8. 哈希(Hash)载荷

哈希载荷包含的是 Hash 验证函数产生的数据,该函数是 SA 协商过程中双方协商出来的 Hash 函数。Hash 数据一般用于验证包含在 ISAKMP 报文中的其余部分数据的完整性,或者对协商实体进行鉴别。

9. 签名载荷(signature)

签名载荷包含由数字签名函数所产生的数据,该函数是 SA 协商过程中双方协商出来的。此载荷用来认证 ISAKMP 报文的完整性,还可用作不可否认服务。

10. Nonce 载荷

Nonce 载荷包含在交换期间用于保证存活和防止重放攻击的随机数。如果 Nonce 用于特殊的密钥交换协议,Nonce 载荷的使用将由该密钥交换机制来指定。Nonce 可作为密钥交换载荷的交换数据的一部分,或作为一个独立的载荷发送。具体如何发送,由密钥交换来定义,而不是 ISAKMP。

11. 通知载荷(notification)

通知载荷用于告知对方一些信息,例如错误状态。

12. 删除载荷(delete)

通信一方利用删除载荷告诉对方自己已经从 SAD 中删除给定 IPSec 协议(IAKMP、AH 或者 ESP)的 SA。注意:删除载荷并不是命令对方删除 SA,而是建议对方删除 SA。如果对方选择忽略该删除载荷,则对方以后再使用该 SA 所发送的报文将失败。另外,对于该删除报文不需要对方应答,也就是说对方不需要返回删除是否成功的报文。

13. 厂商 ID 载荷(Vendor ID)

厂商 ID 载荷用于传输厂商定义的常数。这个机制允许厂商在维持向后兼容性的同

时，试验新的特性。

10.4.5　ISAKMP 协商阶段

ISAKMP 的协商过程分为两个阶段：阶段 1 和阶段 2。两个阶段所协商的对象不同，但协商过程的交换方式（见 10.4.6 小节）是由 ISAKMP 定义的或者由密钥交换协议（如 IKE）定义的。

（1）阶段 1

这个阶段要协商的 SA 可以称为 ISAKMP SA（在 IKE 中可以称为 IKE SA），该 SA 是为了保证阶段 2 的安全通信。

（2）阶段 2

这个阶段要协商的 SA 是密钥交换协议最终要协商的 SA，当 IKE 为 IPSec 协商时可以称为 IPSec SA，是保证 AH 或者 ESP 的安全通信。阶段 2 的安全由阶段 1 的协商结果来保证。阶段 1 所协商的一个 SA 可以用于协商多个阶段 2 的 SA。

10.4.6　交换类型

ISAKMP 定义了 5 种交换类型。交换类型定义的是在通信双方所传送的载荷的类型和顺序，比如一方先发送什么载荷，另一方应如何应答等。这些交换模式的区别在于对传输信息的保护程度不同，并且传输的载荷多少也不同。5 种交换类型分别是：

（1）基本交换（Base Exchange）。

（2）身份保护交换（Identity Protection Exchange）。

（3）纯认证交换（Authentication Only Exchange）。

（4）积极交换（Aggressive Exchange）。

（5）信息交换（Informational Exchange）。

10.5　IKE 协议

1. IKE 概述

IKE 是一种混合型协议，由 RFC2409 定义，包含了 3 个不同协议的有关部分：ISAKMP、Oakley 和 SKEME。IKE 和 ISAKMP 的不同之处在于：IKE 真正定义了一个密钥交换的过程，而 ISAKMP 只是定义了一个通用的可以被任何密钥交换协议使用的框架。

IKE 为 IPSec 通信双方提供密钥材料，这个材料用于生成加密密钥和验证密钥。另外，IKE 也为 IPSec 协议 AH 和 ESP 协商 SA。

IKE 中有 4 种身份认证方式：

（1）基于数字签名（Digital Signature），利用数字证书来表示身份，利用数字签名算法计算出一个签名来验证身份。

（2）基于公开密钥（Public Key Encryption），利用对方的公开密钥加密身份，通过检

查对方发来的该 HASH 值作认证。

(3) 基于修正的公开密钥(Revised Public Key Encryption),对上述方式进行修正。

(4) 基于预共享字符串(Pre-Shared Key),双方事先通过某种方式商定好一个双方共享的字符串。

2 IKE 交换模式

IKE 目前定义了 4 种模式:主模式、积极模式、快速模式和新组模式。前面 3 个用于协商 SA,最后一个用于协商 Diffie-Hellman 算法所用的组。主模式和积极模式用于第一阶段;快速模式用于第二阶段;新组模式用于在第一个阶段后协商新的组。

10.6 本章小结

IPSec 是用于保护 IP 层通信安全的机制,由若干 RFC 文件和 Internet 草案进行定义,而不是一个单独的协议。

安全策略用于定义对数据包的处理方式,存储在安全策略数据库中;IPSec 双方利用安全联盟中的参数对需要进行 IPSec 处理的包进行 IPSec 处理,安全联盟存储在安全联盟数据库中。

传输模式和隧道模式的区别在于保护的对象不同,传输模式要保护的内容是 IP 包的载荷,而隧道模式要保护的是整个 IP 包。

对 IP 包进行的 IPSec 处理有两种:AH 和 ESP。AH 提供无连接的数据完整性、数据来源验证和抗重放攻击服务;而 ESP 除了提供 AH 的这些功能外,还可以提供对数据包加密和数据流量加密。虽然 AH 和 ESP 都提供验证服务,但 AH 的验证范围要比 ESP 更大,包含了源和目的 IP 地址,因此造成了 AH 协议和 NAT 的冲突,而 ESP 则不存在这种问题。

IKE 协议由 3 种协议混合而来:ISAKMP、Oakley 和 SKEME。ISAKMP 协议为 IKE 提供了密钥交换和协商的框架;Oakley 提供了组的概念;SKEME 定义了验证密钥交换的一种类型。

IKE 协议的密钥交换采用 Diffie-Hellman 算法;IKE 协议有 4 种模式:主模式、积极模式、快速模式和新组模式。

习　题

1. IPSec 协议和(　)VPN 隧道协议处于同一层。

   A. PPTP　　B. L2TP　　C. GRE　　D. 以上皆是

2. AH 协议中必须实现的验证算法是(　)。

   A. HMAC-MD5 和 HMAC-SHA1　　B. NULL

   C. HMAC-RIPEMD-160　　D. 以上皆是

3. ESP 协议中不是必须实现的验证算法的是(　)。

A. HMAC-MD5　　B. HMAC-SHA1

C. NULL　　D. HMAC-RIPEMD-160

4. ESP 协议中必须实现的加密算法是(　)。

A. 仅 DES-CBC　　B. 仅 NULL

C. DES-CBC 和 NULL　　D. 3DES-CBC

5. (　)协议必须提供验证服务。

A. AH　　B. ESP　　C. GRE　　D. 以上皆是

6. IKE 协商的第一阶段可以采用(　)。

A. 主模式、快速模式　　B. 快速模式、积极模式

C. 主模式、积极模式　　D. 新组模式

7. IKE 协议由(　)协议混合而成。

A. ISAKMP、Oakley、SKEME　　B. AH、ESP

C. L2TP、GRE　　D. 以上皆不是

8. 下列协议中,(　)协议的数据可以受到 IPSec 的保护。

A. TCP、UDP、IP　　B. ARP　　C. RARP　　D. 以上皆可以

9. 为什么 AH 协议和 NAT 冲突?

10. 简述 IKE 协议的几种模式,以及每一种模式的作用和特点。

第11章 黑客技术

本章要点:

- 黑客攻击的动机;
- 黑客攻击的流程;
- 黑客攻击使用的主要方法和技巧;
- 针对不同网络的攻击方法。

11.1 黑客的动机

黑客的动机究竟是什么?在回答这个问题前,应对黑客的种类有所了解,原因是不同种类的黑客动机有着本质的区别。从黑客行为上划分,黑客有"善意"与"恶意"两种,即所谓的白帽(White Hat)及黑帽(Black Hat)。白帽利用他们的技能做一些善事,而黑帽则利用他们的技能做一些恶事。白帽长期致力于改善计算机社会及其资源,为了改善服务质量及产品,他们不断寻找弱点及脆弱性并公布于众。例如,为了找出程序的安全漏洞,帮助生产厂家改进他们的产品,白帽做了大量的安全上的测试工作。他们所做的工作实际上是一种公众测试形式。与白帽的动机相反,黑帽主要从事一些破坏活动,从事的是一种犯罪行为。大量的案例分析表明黑帽具有以下主要犯罪动机。

(1) 好奇心

许多黑帽声称,他们只是对计算机及电话网感到好奇,希望通过探究这些网络更好地了解它们是如何工作的。

(2) 个人声望

通过破坏具有高价值的目标以提高在黑客社会中的可信度及知名度。

(3) 智力挑战

为了向自己的智力极限挑战或为了向他人炫耀,证明自己的能力,他们热衷于黑客的传说。将自己想像成网络上无所不能的骑士与国王。将网络入侵作为寻求刺激的最佳方法。

(4) 窃取情报

在Internet上监视个人、企业及竞争对手的活动信息及数据文件,以达到窃取情报的目的。

(5) 报复

计算机罪犯感到其雇主本该提升自己、增加薪水或以其他方式承认他的工作。计算

机犯罪活动成为他反击雇主的方法，也希望借此引起别人的注意。

（6）获取非法利益

有相当一部分计算机犯罪是为了赚取金钱。网络与现实的相关性不断地增大，使得盗窃、抢劫这种现实中的犯罪行为在网络中以新的形式出现。他们攻击与利益相关的网站（银行、购物、稀缺资源提供者）非法获取利益；盗窃他人的虚拟资产（账户盗用），给网络金融和网络社区都造成了很大的威胁。

（7）政治目的

任何政治因素都会反映到网络领域。主要表现有：①敌对国之间利用网络的破坏活动；②个人及组织对政府不满而产生的破坏活动。这类黑帽的动机不是钱，几乎永远都是为政治，一般采用的手法包括更改网页、植入计算机病毒等。

11.2　黑客攻击的流程

尽管黑客攻击系统的技能有高低之分，入侵系统手法多种多样，但他们对目标系统实施攻击的流程却大致相同。其攻击过程可归纳为以下 9 个步骤：踩点（foot printing）、扫描（scanning）、查点（enumeration）、获取访问权（gaining access）、权限提升（escalating privilege）、窃取（pilfering）、掩盖踪迹（covering track）、创建后门（creating back doors）和拒绝服务攻击（denial of services）。黑客攻击流程如图 11-1 所示。

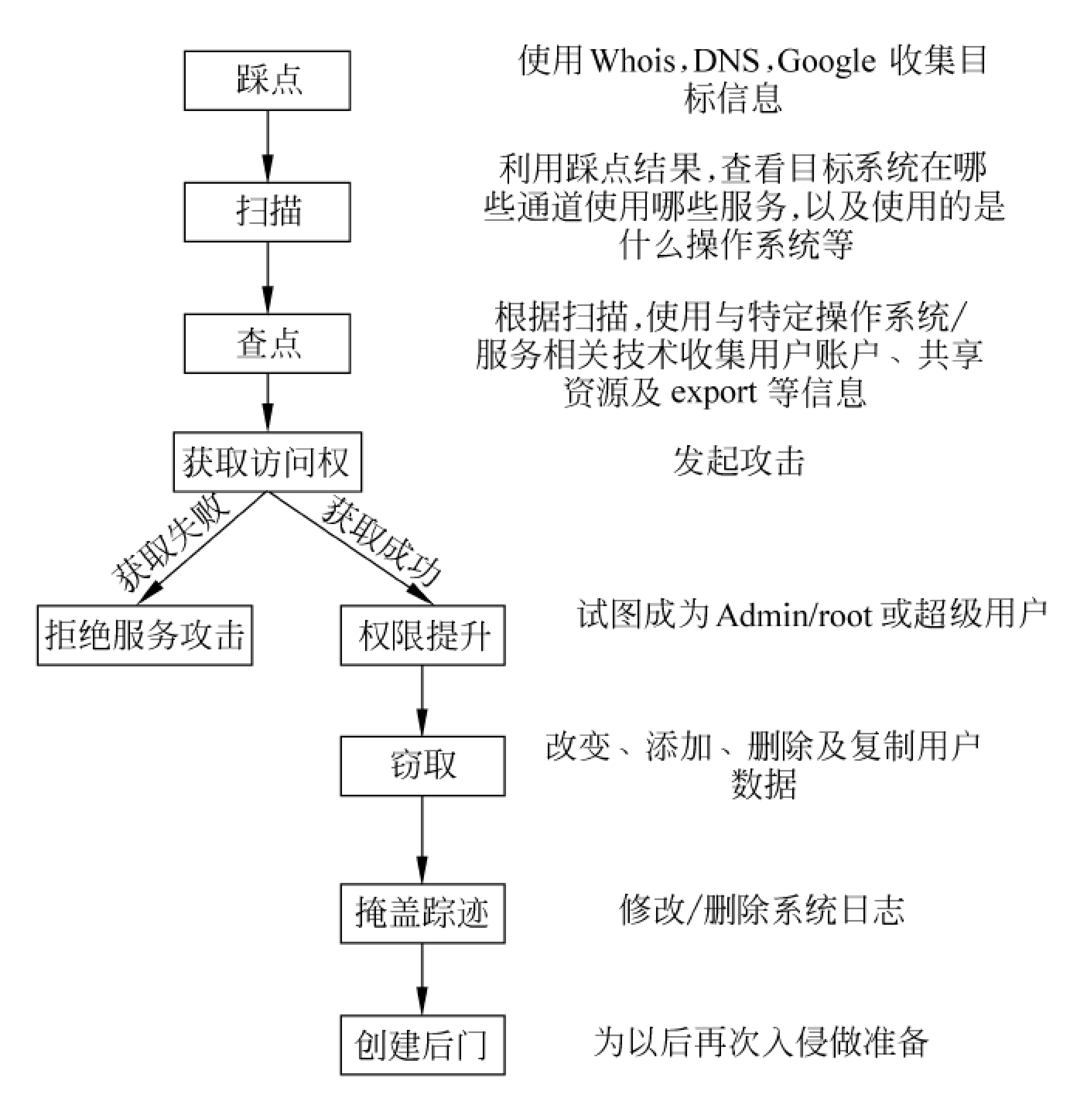


图 11-1　黑客攻击流程图

11.2.1 踩点

“踩点”原意为策划一项盗窃活动的准备阶段。举例来说，当盗贼决定抢劫一家银行时，他们不会大摇大摆地走进去直接要钱，而是狠下一番工夫来搜集这家银行的相关信息，包括武装押运车的路线及运送时间、摄像头的位置、逃跑出口等信息。在黑客攻击领域，“踩点”是传统概念的电子化形式。“踩点”的主要目的是获取目标的如下信息：

- 因特网网络域名、网络地址分配、域名服务器、邮件交换主机和网关等关键系统的位置及软硬件信息。
- 内联网与 Internet 内容类似，但主要关注内部网络的独立地址空间及名称空间。
- 远程访问模拟/数字电话号码和 VPN 访问点。
- 外联网与合作伙伴及子公司的网络的连接地址、连接类型及访问控制机制。
- 开放资源未在前 4 类中列出的信息，例如 Usenet、雇员配置文件等。

为达到以上目的，黑客常采用以下技术。

1. 开放信息源搜索

通过一些标准搜索引擎，揭示一些有价值的信息。例如，通过使用 Usenet 工具检索新闻组（newsgroup）工作帖子，往往能揭示许多有用的东西。通过使用 Google 检索 Web 的根路径 C：\\Inetpub，揭示出目标系统为 Windows NT/2000。对于一些配置过于粗心大意的服务器，利用搜索引擎甚至可以获得 passwd 等重要的安全信息文件。

2 whois 查询

whois 是目标 Internet 域名注册数据库。目前，可用的 whois 数据库很多，例如，查询 com，net，edu 及 org 等结尾的域名可通过 http：//www. networksolutions. com 得到，而查询美国以外的域名则应通过查询 http://www. allwhois. com 得到相应 whois 数据库服务器的地址后完成进一步的查询。通过对 whois 数据库的查询，黑客能够得到以下用于发动攻击的重要信息：

- 注册机构，得到特定的注册信息和相关的 whois 服务器；
- 机构本身，得到与特定目标相关的全部信息；
- 域名，得到与某个域名相关的全部信息；
- 网络，得到与某个网络或 IP 相关的全部信息；
- 联系点（POC），得到与某个人（一般是管理联系人）的相关信息。

例如，下面是通过 http://www. networksolutions. com 查询到的 IBM 公司的信息。

```
Registrant:
IBM Corporation (IBM-DOM)
Old Orchard Rd.
Armonk,NY 10504
US
Domain Name: IBM.COM
Administrative Contact,Technical Contact:
Trio, Nicholas R(SZFHGULFPI)nrt@WATSON.IBM.COM
```

```
PO BOX 218
YORKTOWN HTS,NY10598-0218
US
(914) 945-1850 123 123 1234
Record expires on 20-Mar-2005.
Record created on 19-Mar-1986.
Database last updated on 8-May-2003 21:18:57 EDT.
Domain servers in listed order:
NS.WATSON.IBM.COM129.34.20.80
NS.ALMADEN.IBM.COM198.4.83.35
NS.AUSTIN.IBM.COM192.35.232.34
NS.ERS.IBM.COM204.146.173.35
```

3. DNS 区域传送

DNS 区域传送是一种 DNS 服务器的冗余机制。通过该机制,辅 DNS 服务器能够从其主 DNS 服务器更新自己的数据,以便主 DNS 服务器不可用时,辅 DNS 服务器能够接替主 DNS 服务器工作。正常情况下,DNS 区域传送操作只对辅 DNS 服务器开放。然而,当系统管理员配置错误时,将导致任何主机均可请求主 DNS 服务器提供一个区域数据的备份,以致目标域中所有主机信息泄露。能够实现 DNS 区域传送的常用工具有 dig,nslookup 及 Windows 版本的 Sam Spade(其网址为 http://www.samspade.org)。

11.22　扫描

通过踩点已获得一定信息(IP 地址范围、DNS 服务器地址和邮件服务器地址等),下一步需要确定目标网络范围内哪些系统是“活动”的,以及它们提供哪些服务。与盗窃案之前的踩点相比,扫描就像是辨别建筑物的位置并观察它们有哪些门窗。扫描的主要目的是使攻击者对攻击的目标系统所提供的各种服务进行评估,以便集中精力在最有希望的途径上发动攻击。

扫描中采用的主要技术有 Ping 扫射(Ping Sweep)、TCP/UDP 端口扫描、操作系统检测及旗标(banner)的获取。

1. Ping 扫射

Ping 扫射是判别主机是否“活动”的有效方式。Ping 用于向目标主机发送 ICMP 回射请求(Echo Request)分组,并期待由此引发的表明目标系统“活动”的回射应答(Echo Reply)分组。常用的 Ping 扫射工具有操作系统的 Ping 命令及用于扫射网段的 fping,WS_ping 等。

2 端口扫描

端口扫描就是连接到目标机的 TCP 和 UDP 端口上,确定哪些服务正在运行及服务的版本号,以便发现相应服务程序的漏洞。著名的扫描工具有 UNIX 系统上运行的 Netcat(http://www.atstake.com/research/tools/network utilities)及 Nmap(http://www.insecure.org/nmap),Windows 系统上运行的 superscan(http://www.webattack.com/get/

superscan.shtml)及 NetScan Tool Pro 2003(http://www.nwpsw.com)。

3. 操作系统检测

由于许多漏洞是和操作系统紧密相关的，因此，确定操作系统类型对于黑客攻击目标来说也十分重要。目前用于探测操作系统的技术主要可以分为两类：利用系统旗标信息和利用 TCP/IP 堆栈指纹。每种技术进一步细分为主动鉴别及被动鉴别。目前，常用的检测工具有 Nmap，Queso (http://www.apostols.org/projectz/queso) 和 Siphon (http://siphon.datanerds.net)。

4. 旗标获取

最后一种扫描手段是旗标获取。在旗标获取方法中，使用一个打开端口来联系和识别系统提供的服务及版本号。最常用的方法是连接到一个端口，按 Enter 键几次，看返回什么类型的信息。

例如：

```
\[Netat_svr# \] Telnet 192.168.5.33 22
SSH-1.99-OpenSSH_3.1p1
```

表明该端口提供 SSH 服务，版本号为 3.1p1。

5. 安全措施探查

目前，重要的网络服务器一般都会配置安全防护设备。基本的有防火墙、入侵检测。还有一些重要的安全服务器会配置更多的安全防护装置，如蜜罐系统、防 DoS 攻击系统和邮件过滤等。在扫描过程中根据扫描结果，需要判断目标使用了哪些安全防护措施。获取的内容包括：

① 获取目标的网络路径信息。

- 目标网段信息：确认目标所在的网段，掩码情况。判断安全区域划分情况。为可能的跳板攻击做准备。
- 目标路由信息：确认目标的具体路由情况，判断在路由路径上的各个设备类型。如是路由器、三层交换机或防火墙。

② 了解目标前架设的安全设备的情况，确认目标是否安装了安全设施。一般对攻击影响较大的包括防火墙、入侵检测和蜜罐系统等。

③ 了解目标使用安全设备情况。这对攻击的隐蔽性影响很大，同时也决定了在后期安装后门的困难程度。这部分主要包括入侵检测、日志审计及防病毒安装情况。

安全措施探查主要通过分析扫描数据总结出来。一般通过分析简单攻击是否存在阻断行为，可以确认是否在关键路径上存在动态安全防护设备，检查 icmp 及端口扫描反馈数据，可以确认是否存在防火墙等包过滤设备。通过检查数据重定向情况，可以猜测服务器真实 IP 地址及通路设置情况。通过伪装病毒通信可以检查是否存在蜜罐系统。

11.2.3　查点

通过扫描，入侵者掌握了目标系统所使用的操作系统，下一步工作是查点。查点就是

搜索特定系统上用户和用户组名、路由表、SNMP 信息、共享资源、服务程序及旗标等信息。查点所采用的技术依操作系统而定。

在 Windows 系统上主要采用的技术有"查点 NetBIOS"线路、空会话(Null Session)、SNMP 代理和活动目录(Active Directory)等。Windows 系统上主要使用以下工具：

(1) Windows 系统命令

net view,nbtstat,nbtscan 及 nltest。

(2) 第三方软件

Netviewx(http://www.ibt.ku.dk/jesper/NetViewX/default.htm);
Userdump(http://www.hammerofgod.com/download.htm);
User2sid(http://www.ntbugtraq.com);
GetAcct(http://securityfriday.com);
DumpSec(http://www.somarsoft.com);
Legion(http://www.legionlan.com);
NAT(http://www.hackingexposed.com)。

在 UNIX 系统上采用的技术有 RPC 查点、NIS 查点、NFS 查点及 SNMP 查点等。UNIX 系统上常用的工具有 rpcinfo，rpcdump，showmount，finger，rwho，ruser，nmap，telnet，nc 及 snmpwalk 等。

11.24　获取访问权

在搜集到目标系统的足够信息后，下一步要完成的工作自然是得到目标系统的访问权进而完成对目标系统的入侵。对于 Windows 系统采用的主要技术有 NetBIOS SMB 密码猜测(包括手工及字典猜测)、窃听 LM 及 NTLM 认证散列、攻击 IIS Web 服务器及远程缓冲区溢出。而 UNIX 系统采用的主要技术有蛮力密码攻击，密码窃听，通过向某个活动的服务发送精心构造的数据，以产生攻击者所希望的结果的数据驱动式攻击(例如缓冲区溢出、输入验证和字典攻击等)，RPC 攻击，NFS 攻击及针对 X Window 系统的攻击等。著名的密码窃听工具有 sniffer pro(http://www.sniffer.com)，TCPdump，LC4(L0phtcrack version 4，http://www.atstake.com/research/lc/)和 readsmb。字典攻击工具有 LC4，John the RIPper(http://www.openwall.com/john)，NAT，SMBGrind(http://www.nai.com)及 fgrind。对于对访问限制的服务，通过暴力破解的方式，一般都能在可接受的时间内获取到访问权限。

11.25　权限提升

一旦攻击者通过前面 4 步获得了系统上任意普通用户的访问权限后，攻击者就会试图将普通用户权限提升至超级用户权限，以便完成对系统的完全控制。这种从一个较低权限开始，通过各种攻击手段得到较高权限的过程称为权限提升。权限提升所采取的技术主要有通过得到的密码文件，利用现有工具软件，破解系统上其他用户名及口令；利用不同操作系统及服务的漏洞(如 Windows 2000 NetDDE 漏洞)，利用管理员不正确的系统配置等。常用的口令破解工具有 John The RIPper，John The RIPper，得到 Windows

NT 管理员权限的工具有 lc_message，getadmin，sechole，Invisible Keystroke Logger（http：//www.amecisco.com/iksnt.htm）。

11.26　窃取

一旦攻击者得到了系统的完全控制权，接下来将完成的工作是窃取，即进行一些敏感数据的篡改、添加、删除及复制（例如 Windows 系统的注册表、UNIX 系统的 rhost 文件等）。通过对敏感数据的分析，为进一步攻击应用系统做准备。

11.27　掩盖踪迹

黑客并非踏雪无痕，一旦黑客入侵系统，必然留下痕迹。此时，黑客需要做的首要工作就是清除所有入侵痕迹，避免自己被检测出来，以便能够随时返回被入侵系统继续干坏事或作为入侵其他系统的中继跳板。掩盖踪迹的主要工作有禁止系统审计、清空事件日志、隐藏作案工具及使用人们称为 rootkit 的工具组替换那些常用的操作系统命令。常用的清除日志工具有 zap，wzap 和 wted。

11.28　创建后门

黑客的最后一招便是在受害系统上创建一些后门及陷阱，以便入侵者一时兴起时，卷土重来，并能以特权用户的身份控制整个系统。创建后门的主要方法有创建具有特权用户权限的虚假用户账号、安装批处理、安装远程控制工具、使用木马程序替换系统程序、安装监控机制及感染启动文件等。黑客常用的工具有 rootkit、sub7（http：//www.sub7.net）、cron、at、UNIX 的 rc、Windows 启动文件夹、Netcat（http：//www.atstake.com/research/tools）、VNC（http：//www.realvnc.com）、BO2K（http：//sourceforge.net/projects/bo2k）、secadmin、Invisible Keystroke Logger、remove.exe 等。

11.29　拒绝服务攻击

如果黑客未能成功地完成第 4 步的获取访问权，那么他们所能采取的最恶毒的手段便是进行拒绝服务攻击。即用精心准备好的漏洞代码攻击系统使目标服务器资源耗尽或资源过载，以致没有能力再向外提供服务。攻击所采用的技术主要是利用协议漏洞及不同系统实现的漏洞。

11.3　黑客技术概述

网络是多种信息技术的集合体，它的运行依靠相关的大量技术标准和协议。作为网络的入侵者，黑客的工作主要是通过对技术和实际实现中的逻辑漏洞进行挖掘，通过系统允许的操作对没有权限操作的信息资源进行访问和处理。目前，黑客对网络的攻击主要是通过网络中存在的拓扑漏洞及对外提供服务的实现漏洞实现成功的渗透。除了使用这些技术上的漏洞，黑客还可以充分利用人为运行管理中存在的问题对目标网络实施入侵。

通过欺骗、信息搜集等社会工程学的方法，黑客可以从网络运行管理的薄弱环节入手，通过对人本身的习惯的把握，迅速地完成对网络用户身份的窃取并进而完成对整个网络的攻击。

可以看出，黑客的技术范围很广，涉及网络协议解析、源码安全性分析、密码强度分析和社会工程学等多个不同的学科。入侵一个目标系统，在早期需要黑客具有过硬的协议分析基础、深厚的数学功底。但由于网络的共享能力及自动攻击脚本的成熟与广泛的散播，现在黑客的行为越演越烈，而对黑客的技术要求也在不断地降低。

目前，在实施网络攻击中，黑客所使用的入侵技术主要包括以下几种：

- 协议漏洞渗透；
- 密码分析还原；
- 应用漏洞分析与渗透；
- 社会工程学；
- 拒绝服务攻击；
- 病毒或后门攻击。

11.3.1　协议漏洞渗透

网络中包含着种类繁多但层次清晰的网络协议规范。这些协议规范是网络运行的基本准则，也是构建在其上的各种应用和服务的运行基础。但对于底层的网络协议来说，对于安全的考虑有着先天的不足，部分网络协议具有严重的安全漏洞。通过对网络标准协议的分析，黑客可以从中总结出针对协议的攻击过程，利用协议的漏洞实现对目标网络的攻击。

随着网络的不断发展，网络安全越来越得到管理者的重视，大量陈旧的网络协议被新的更安全的网络协议所代替。作为现代网络的核心协议，TCP/IP 协议正在不断地得到安全的修补，即在不破坏正常协议流程的情况下，修改影响网络安全的部分。当然，由于先天的不足，一些协议上的漏洞是无法通过修改协议弥补的。通过应用这些固有的协议漏洞，黑客开发出了针对特定网络协议环境下的网络攻击技术，这些技术以会话侦听与劫持技术和地址欺骗技术应用较多。

1. 会话侦听与劫持技术

传统的以太网络使用共享的方式完成对数据分组的传送。这在目前尤其在一些已经有一定历史的网络中是主要的分组发送方式。在这种方式下，发往目的结点的分组数据实际上被发送给了所在网段的每一个结点。目的结点接收这些分组，并与其他结点共享传送带宽。虽然从带宽的利用率上，这样做的实现利用率并不高，但由于实际的实现较为简单，同时造价较低，因此在网络中得到了广泛的应用。正是根据共享式的网络环境的数据共享特性，黑客技术中出现了会话窃听与劫持技术。

只要可以作为目标网络环境的一个结点，就可以接收到目标网络中流动的所有数据信息。这种接收的设置非常简单，对于普通的计算机，只要将网卡设为混杂模式就可以达到接收处理所有网络数据的目的。利用会话窃听技术，入侵者可以通过重组数据包将网

络内容还原,轻松地获得明文信息。例如,当前的网站登录中,在密码传输方面使用的方式几乎都是明文传送。因此,这类密码也就相当容易获得。由于人的因素,每个人使用的用户名和密码都只限于几个。通过获取明文密码信息,入侵者不但可以轻易地以被监听者的身份进入到各个网站,还可以通过搜集的用户密码表进入被监听人的计算机进行破坏。

会话窃听技术是网络信息搜集的一种重要方式,而利用 TCP 协议的漏洞,黑客更可以对所窥探的 TCP 连接进行临时的劫持,以会话一方用户的身份继续进行会话。会话劫持的根源在于 TCP 协议中对分组的处理。

2 地址欺骗技术

在传统的网络中,存在着大量的简单认证方式,这些方式的基本原则就是以主机的 IP 地址作为认证的基础,即所谓的主机信任。通过设定主机信任关系,用户对网络的访问和管理行为变得简单,很大程度上提高了网络的易用性。

这样的认证行为基于以下网络协议原则,即在网络中,所有的计算机都是通过如 IP 这样的地址进行辨认,每一个主机具有固定的并且是唯一(这里的唯一相对于所在网络而言)的地址。通过确认 IP 就可以确认目标主机的身份。但就像现实中有假的身份证一样,网络的地址也可以被假冒,这就是所谓 IP 地址的欺骗。由于网络的基础协议在安全性上的漏洞,这种假冒远较现实中的假冒方便简单。通过对地址的假冒,入侵者可以获得所仿冒地址计算机的所有特权,也就容易攻入到其他给被仿冒计算机提供信任连接的计算机上,造成机密泄露。如果防火墙配置不当,这种攻击甚至可以绕过防火墙,破坏防火墙内的计算机。

11.3.2　密码分析还原

为了保证数据的安全性,现在通常的方法是对数据进行加密,防止可疑的截取行为造成的信息泄露。对于数据的加密通常需要一个密钥,数据与密钥通过加密算法自动机进行合成,生成密文。对于不知道密钥的攻击者来说,截获的密文难以理解。而对于非对称加密算法,即使攻击者知道密钥,也无法从密文中还原出明文信息。这样就可以保证网络通信信息的安全性。同样,对于认证用的密码信息,一般也是使用强度较高的加密算法进行加密,以密文的形式存储在系统中。这些密文使用加密算法的强度一般较高,黑客即使获得密文存储文件,也难以从这些密文中分析出正确的密码。

密码学等加密技术向人们做出保证,密码的攻破理论上是不可行的,如果采用蛮力攻击的话,所用的时间将长到足够保证安全的程度。但现实中,密码的破解却并不如理论中所保证的那样困难。随着计算机运算速度的指数级提高,相同的运算量所使用的时间明显地缩短。同时,对加密算法的强度分析以及社会工程学的密码筛选技术的不断发展,现实网络中的大量密码可以在可接受的时间内被分析还原。密码分析与还原技术不使用系统和网络本身的漏洞,虽然涉及对密码算法的强度分析,但它主要利用的是人的惰性及系统的错误配置。应用这类技术手段攻击通常是可以通过人工手段避免的,只要严格要求网络所在用户的密码强度,还是可以避免大部分的攻击,但由于这涉及人员管理,代价也

非常大。

目前网络中使用的加密算法，从加密的种类上来分，主要包括对称加密和非对称加密两种基本的类别。根据分析的出发点不同，密码分析还原技术主要分为密码还原技术和密码猜测技术。对于网络上通用的标准加密算法来说，攻击这类具有很高强度加密算法的手段通常是使用后一种技术。在进行攻击的时候，密码分析还原所针对的对象主要是通过其他侦听手段获取到的认证数据信息，包括系统存储认证信息的文件或利用连接侦听手段获取的用户登录的通信信息数据。

1. 密码还原技术

密码还原技术主要针对的是强度较低的加密算法。通过对加密过程的分析，从加密算法中找出算法的薄弱环节，从加密样本中直接分析出相关的密钥和明文。对于非对称算法，可以通过对密文的反推将明文的可能范围限定在有限的范围内，达到还原密文的结果。这种方法需要对密码算法有深入的研究，同时，相关算法的密码还原过程的出现，也就注定了相应加密算法寿命的终结。对于目前网络上通行的标准加密算法来说，从理论和实践中还没出现对应的密码还原过程，因此密码还原技术的使用并不多。但对于没有公开加密算法的操作系统来说，由于算法的强度不够，在过程被了解后，黑客就会根据分析中获得的算法漏洞完成密码还原的算法。现在，对于 Windows 操作系统来说，用户认证的加密算法就已经被分析攻破，用户只要使用密码破解程序就可以完成对系统上所有密码的破解，获取系统上所有用户的访问权限。

2 密码猜测技术

密码还原技术需要目标系统使用强度不高的、有一定安全漏洞的加密算法，而对于一般的成熟加密算法，密码攻击主要使用的是密码猜测技术。密码猜测技术的原理主要是利用穷举的方法猜测可能的明文密码，将猜测的明文经过加密后与实际的密文进行比较，如果所猜测的密文与实际的密文相符，则表明密码攻击成功，攻击者可以利用这个密码获得相应用户的权限。往往这样猜测出来的密码与实际的密码相一致。

密码猜测技术的核心在于如何根据已知的信息调整密码猜测的过程，在尽可能短的时间内破解密码。从理论上讲，密码猜测的破解过程需要一段很长的时间，而实际上，应用密码猜测技术实现对系统的攻击是目前最为有效的攻击方式。这种方法比想像的更加有效的原因是许多人在选择密码时，技巧性都不是很好，密码复杂性不高。简单的密码非常容易猜到，例如，很多人使用用户名加上一些有意义的数字（生日或是连续数字序列等）作为自己的密码，甚至有些人的密码与用户名相同，一些密码长度只有几个甚至一个字符。这类密码容易记忆，但也方便了入侵者。

密码猜测技术就是利用人们的这种密码设置习惯，针对所搜集到的信息，对有意义的单词和用户名与生日形式的数列代码或简单数字序列进行排列组合，形成密码字典，同时根据所搜集到的用户信息，对字典的排列顺序进行调整。以这个生成的字典作为基础，模拟登录的方式，逐一进行匹配操作，密码猜测工具可以利用这种方式破解大量的系统。密码猜测技术的核心就是这种密码字典的生成技术。上述的生成方式是密码字典的基本生成原则。例如，根据目标网络所在的物理位置，人员的国籍、姓名和性格等信息，密码猜测

工具可以将与信息相关的单词选取出来形成更小的单词组合，而根据人员的年龄、电话等信息，密码猜测工具可以将数字序列集限定在更小的范围内。这样组合出来的字典更小，针对性更强，可以实现更快速度的破解。随着对目标网络用户信息搜集的深入，密码猜测工具对字典进行的筛选越来越精细，字典序列调整的依据也就越多。对于攻击用的密码猜测技术，其主要目的就是为了获取对目标网络的访问权限，它是黑客入侵过程中介于信息搜集和攻击之间的攻击过程。从对目标网络的密码猜测攻击中就可以了解到目标网络对安全的重视程度。在以往黑客攻击的事件中，有大量目标网络由于不重视安全管理，用户的密码强度不够，黑客可以在几分钟甚至几秒钟的时间内破解大量一般用户甚至是管理员账户的密码。

11.3.3　应用漏洞分析与渗透

任何的应用程序都不可避免地存在逻辑漏洞，这在 IT 行业中已经形成了共识。这一点，对于安全隐患也同样适用。在这方面操作系统也不例外，几乎每天都有人宣布发现了某个操作系统的安全漏洞，而这些安全漏洞也就成为了入侵者的攻击对象。通过对这些安全漏洞的分析，确认漏洞的引发方式以及引发后对系统造成的影响，攻击者可以使用合适的攻击程序引发漏洞的启动，破坏整个服务系统的运行过程，进而渗透到服务系统中，造成目标网络的损失。

目前，对各个网站的攻击几乎都使用到了应用漏洞分析与渗透技术，攻击者或是利用 WWW 服务器的漏洞，或是利用操作系统的缺陷攻入服务器，篡改网站主页。最近经常提及的对微软的 IIS 服务器的攻击，就是利用 IIS 对 unicode 解释的缺陷实现的。由于这类错误，入侵者甚至只使用浏览器就可以随意地篡改网站服务器的内容。最新的病毒 Nimda 也是利用了 Outlook Express 的安全漏洞迅速地传播开来的。

应用漏洞从错误类型上主要包括服务流程漏洞和边界条件漏洞。

1. 服务流程漏洞

服务流程漏洞指服务程序在运行处理过程中，由于流程次序的颠倒或对意外条件的处理的随意性，造成用户有可能通过特殊类型的访问绕过安全控制部分或使服务进入到异常的运行状态。例如，著名的 IIS 漏洞就是由 unicode 的解释过程在路径安全确认过程之后这样的流程错误产生的。利用这种流程错误，用户可以将路径分割符分解为 unicode 编码中的两个字符，造成服务在确认路径的时候被误认为属于文件名而分析通过，在经过 unicode 解释后，系统根据指定的路径达到了对系统非公开资源的非法访问。又如用户可以对处理输入不严密的 CGI 程序输入含有运行代码的请求，如果没有对输入进行合法性的处理，CGI 程序就会在执行的过程中启动用户写入的运行代码，造成系统信息的泄露或破坏。

2 边界条件漏洞

边界条件漏洞则主要针对服务程序中存在的边界处理不严谨的情况。在对服务程序的开发过程中，很多边界条件尤其是对输入信息的合法性处理往往很难做到周全，在正常情况下，对边界条件考虑的不严密并不会造成明显可见的错误，但这种不严密的处理却会

带来严重的安全隐患。在边界漏洞中，以内存溢出错误最为普遍，影响也最为严重。有很多攻击都是利用超长的数据填满数据区并造成溢出错误，利用这种溢出在没有写权限的内存中写入非法数据。这些数据有些只是单纯地造成相关服务的停止，而另一些则带有可运行信息，通过溢出，重定向了返回指针，启动写入数据中的运行代码，获取远程操作系统的超级管理员权限或是对数据进行破坏，造成服务甚至整个系统的崩溃。由于这种攻击涉及系统内核和内存分配，与操作系统直接相关，但往往非常有效，并且很难杜绝。这种类型的攻击是目前应用最多的攻击方式，对于网络的影响也最为严重。这类攻击包括BIND 溢出攻击、sendmail 溢出攻击和 Linux bash 缓冲溢出攻击等。随着应用程序的复杂性不断提高，边界条件类型的漏洞将会不断出现，而基于这种漏洞的攻击也会不断增加。

11.3.4　社会工程学

社会工程学与黑客使用的其他技术具有很大的差别，它所研究的对象不是严谨的计算机技术，而是目标网络的人员。社会工程学主要是利用说服或欺骗的方法来获得对信息系统的访问。这种说服和欺骗通常是通过和人交流或其他互动方式实现的。

简单地说，社会工程学就是黑客对人类天性趋于信任倾向的聪明利用。黑客的目标是获得信息，通过获得那些重要系统未授权的访问路径来获取该系统中的某些信息。信任是一切安全的基础。一般认为对于保护与审核的信任是整个安全链中最薄弱的一环，人类那种天生愿意相信其他人的说辞的倾向让大多数人容易被这种手段所利用。这也是许多很有经验的安全专家所强调的。

可以从两个层次来对社会工程学类的攻击进行分析：物理上的和心理上的。

1. 物理分析

物理上，入侵发生的物理地点可以是工作区、电话、目标企业垃圾堆，甚至是在网上。

（1）对于工作区来说，黑客可以只是简单地走进来，冒充允许进入公司的维护人员或者顾问。大多数情况下，入侵者可以对整个工作区进行深入的观察，直到找到一些密码或是一些可以利用的资料之后离开。另一种获得审核信息的手段就是站在工作区观察公司雇员如何输入密码并偷偷记住。

（2）最流行的社会工程学手段是通过电话进行的。黑客可以冒充一个权力很大或者很重要的人物的身份，打电话从其他用户那里获得信息。一般机构的咨询台容易成为这类攻击的目标。咨询台之所以容易受到社会工程学的攻击，是因为他们所处的位置就是为他人提供帮助的，因此就可能被人利用来获取非法信息。咨询台人员一般接受的训练都是要求他们待人友善，并能够提供别人所需要的信息，所以这就成为了社会工程学家们的金矿。大多数的咨询台人员所接受的安全领域的培训与教育很少，这就造成了很大的安全隐患。

（3）翻垃圾是另一种常用的社会工程学手段。因为企业的垃圾堆里面往往包含了大量的信息。在垃圾堆中可以找出很多危害安全的信息，包括企业的电话簿、机构表格、备忘录、公司的规定手册、会议时间安排表、事件和假期、系统手册、打印的敏感信息或是登

录名和密码、打印出来的源代码、磁盘和磁带、公司的信件头格式和备忘录的格式，以及废旧的硬件。这些资源可以向黑客提供大量的信息。电话簿可以向黑客提供员工的姓名、电话号码来作为目标和冒充的对象。机构的表格包含的信息可以让他们知道机构中的高级员工的姓名。备忘录中的信息可以让他们一点点地获得有用信息来帮助他们扮演可信任的身份。企业的规定可以让他们了解机构的安全情况如何。日期安排表更是重要，黑客可以知道在某一时间有哪些员工出差不在公司。系统手册、敏感信息，还有其他技术资料可以帮助黑客闯入机构的计算机网络。至于废旧硬件，特别是硬盘，黑客可以对它进行恢复来获取有用信息。

（4）Internet 是使用社会工程学来获取密码的乐园。这主要是因为许多用户都把自己所有账号的密码设置为同一个。所以一旦黑客拥有了其中的一个密码以后，他就获得了多个账号的使用权。黑客常用的一种手段是通过在线表格进行社会工程学攻击。他可以发送某种彩票中奖的消息给用户，然后要求用户输入姓名(以及电子邮件地址，这样他甚至可以获得用户在机构内部使用的账户名)以及密码。这种表格不仅可以以在线表格的方式发送，同样可以使用普通邮件进行发送。况且，如果是使用普通信件方式的话，这些表格看上去就会更加像是从合法的机构中发出的，欺骗的可能性也就更大了。黑客在线获得信息的另一种方法是冒充该网络的管理员，通过电子邮件向用户索要密码。这种方法并不是十分有效，因为用户在线的时候对黑客的警觉性比不在线时要高，但是该方法仍然是值得考虑的。此外，黑客也有可能放置弹出窗口，并让它看起来像是整个网站的一部分，声称是用来解决某些问题的，诱使用户重新输入账号与密码。这时用户一般会知道不应当通过明文来传输密码，但是，即使如此，管理员也应当定期提醒用户防范这种类型的欺骗。如果想做到进一步安全的话，系统管理员应当警告用户，除非是与合法可信的网络工作员工进行面对面交谈；否则任何时候都不能公开自己的密码。

（5）电子邮件同样可以用来作为更直接获取系统访问权限的手段。例如，从某位有信任关系的人那里发来的电子邮件附件中可能携带病毒、蠕虫或者木马。为了攻击目标网络，黑客通常会将包含后门的邮件发送给目标网络中的用户。只要存在缺乏安全防范意识的用户，后门就可能被安装，黑客就获得了一个隐蔽的攻击通道，为下一步攻击更重要的系统做准备。

2 心理分析

除了这些物理手段以外，黑客也可能充分利用用户的心理，从心理学角度进行社会工程学式的攻击。基本的说服手段包括扮演、讨好、同情和拉关系等。不论是使用哪一种方法，主要目的还是说服目标泄露所需要的敏感信息。

（1）扮演一般来讲是构造某种类型的角色并按该角色的身份行事。经常采用的角色包括维修人员、技术支持人员、经理、可信的第三方人员或者企业同事。角色通常是越简单越好。某些时候就仅仅是打电话给目标，索取需要的信息。但是这种方式并不是任何时候都有效。在其他情况下，黑客会专心调查目标机构中的某一个人，并在他外出的时候冒充他的声音来打电话询问信息。

（2）还有一种比较有争议的社会工程学手段是仅仅简单地表现出友善的一面来套取

信息。其理由是大多数人都愿意相信打电话来寻求帮助的同事所说的话。所以黑客只需要获得基本的信任就可以了，稍稍恭维一下目标就会让目标乐意进一步合作。

（3）获得非法信息更为高级的手段称为“反向社会工程学”。黑客会扮演一个不存在的但是权利很大的人物，让企业雇员主动地向他询问信息。如果深入地研究、细心地计划与实施的话，反向社会工程学攻击手段可以让黑客获得更多更好的机会来从雇员那里获得有价值的信息。但是这需要大量的时间来准备，研究及进行一些前期的黑客工作。反向社会工程学包括 3 个部分：暗中破坏，自我推销和进行帮助。黑客先是对网络进行暗中破坏，让网络出现明显的问题，然后对网络进行维修并从雇员那里获得他真正需要的信息。那些雇员不会知道他是个黑客，因为网络中出现的问题得到解决，所有人都会很高兴。

社会工程学的攻击对象是目标网络中的工作人员和目标网络中的运行管理制度。对于人员的安全管理，包括安全知识的培训，其花费往往是巨大的。社会工程学没有或是很少利用目标网络中的技术漏洞，它利用人员对制度实际操作中的灵活性，对目标网络进行渗透。这种攻击技术很难防范，而对于受到这种攻击的企业，由于涉及暴露其自身的制度和管理漏洞，在某种程度上会损害企业的形象，因此也只能自认倒霉。因此，社会工程学作为一种重要的信息搜集的方式，在黑客攻击的踩点阶段被广泛采用。

11.3.5　恶意拒绝服务攻击

拒绝服务攻击最主要的目的是造成被攻击服务器资源耗尽或系统崩溃而无法提供服务。这样的入侵对于服务器来说可能并不会造成损害，但可以造成人们对被攻击服务器所提供服务的信任度下降，影响公司的声誉以及用户对网络服务的使用。这类攻击主要还是利用网络协议的一些薄弱环节，通过发送大量无效请求数据包造成服务器进程无法短期释放，大量积累耗尽系统资源，使得服务器无法对正常的请求进行响应，造成服务的瘫痪。

通过普通的网络连线，使用者传送信息要求服务器予以确定，于是服务器回复用户。用户被确定后，就可登录服务器。“拒绝服务”的攻击方式就是利用了服务器在回复过程中存在的资源占用缺陷，用户将众多要求确认的信息传送到服务器，使服务器里充斥着这种无用的信息。所有的信息都有需回复的虚假地址，以至于当服务器试图回传时，却无法找到用户。根据协议的规定，服务器相关进程会进行暂时的等候，有时超过一分钟，之后才进行进程资源的释放。由于不断地发送这种虚假的连接请求信息，当进入等待释放的进程增加速度远大于系统释放进程的速度时，就会造成服务器中待释放的进程不断积累，最终造成资源的耗尽而导致服务器瘫痪。

最基本的 DoS 攻击就是利用这种合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务器的响应。而 DDoS 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一的方式，当攻击目标 CPU 速度低、内存小或者网络带宽小等各项性能指标不高时，效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了。这样分布式的拒绝服务攻击手段（DDoS）就应运而生

了。它利用大量的傀儡机来发起进攻，用比从前更大的规模来进攻受害者。

高速广域连接的网络给大家带来了方便，也为 DDoS 攻击创造了极为有利的条件。在低速网络时代，黑客占领攻击用的傀儡机时，总是会优先考虑离目标网络距离近的机器，因为经过路由器的跳数少，效果好。而现在电信骨干结点之间的连接都是以 G 为级别的，大城市之间更可以达到 2.5Gbps 的连接，这使得攻击可以从更远的地方或者其他城市发起，攻击者的傀儡机位置可以分布在更大的范围内，选择起来更灵活了。

一个比较完善的 DDoS 攻击体系分成 3 大部分：傀儡控制、攻击用傀儡和攻击目标。傀儡控制和攻击用傀儡分别用作控制和实际发起攻击。对攻击目标来说，DDoS 的实际攻击包是从攻击用傀儡机上发出的，傀儡控制机只发布命令而不参与实际的攻击。对傀儡控制和攻击用傀儡计算机，黑客有控制权（或者部分的控制权），并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自黑客的指令，通常它还会利用各种手段隐藏自己，以图不被别人发现。在平时，这些傀儡机器并没有什么异常，只是一旦黑客与它们连接进行控制，并发出指令的时候，攻击傀儡机就成为害人者去发起攻击了。发起拒绝服务攻击时，黑客通常要进行信息搜集，攻击其他安全强度较低的网络，在被攻击网络的主机中安装傀儡程序作为攻击主机。完成以上工作后，黑客就明确了攻击目标，并组成了 DDoS 攻击体系中的傀儡控制和攻击用傀儡部分，可以进行实际的攻击了。

拒绝服务攻击由于不是使用什么漏洞，目前还没有很好的解决方案，因此也就被恶意的入侵者大量地使用。前面提到的地址欺骗攻击方式中，入侵者一般先要对被仿冒计算机进行拒绝服务攻击，使得被仿冒计算机无法进行正常响应，从而假冒应答完成地址欺骗。

11.3.6　病毒或后门攻击

计算机病毒检测与网络入侵防御在计算机与网络技术不断发展的促进下，出现了需要共同防御的敌人。现在的病毒不仅是通过磁盘才能传播，为了适应网络日益普及的形式，病毒也在自身的传播方式中加入了网络这个可能会造成更大危害的传播介质。为了能够在网络上传播，病毒也越来越多地继承了网络入侵的一些特性，成为一种自动化的软体网络入侵者。它们利用网络入侵技术，通过网络进行广泛的传播渗透，红色代码病毒和 Nimda 病毒就属此类。它们利用网络入侵的方式，侵入计算机并利用被感染计算机，对周围的计算机进行入侵扫描以进一步传播感染其他计算机。有些病毒（或者叫木马）感染计算机，为远程入侵者提供可以控制被感染计算机的后门，著名的冰河病毒就属此类。入侵者通过各种手段，在用户主机上安装后门服务程序，并利用自身的客户程序监视主机的行为，甚至控制主机的操作。

病毒或后门攻击技术主要是漏洞攻击技术和社会工程学攻击技术的综合应用。通常入侵者会利用社会工程学将病毒或后门绕过安全防御体系引入到目标网络内部。在进入到内部后，病毒或后门自身在提供黑客进行访问和攻击的通道的同时，还不断地利用掌握的应用漏洞在目标网络内部进行广泛的散播。由于病毒有很强的自我保护和复制能力，因此，借助于目标网络内部的网络环境，可以迅速感染目标网络中的其他主机。随着现在

用户间数据交换的日益普及,后门和病毒被广泛地传播,对网络的安全及用户的利益造成了极大的危害。

11.4 针对网络的攻击

除了针对不同的操作系统进行攻击外,还有针对网络设备的攻击。物理网络是网络服务的基础,在脆弱的网络上是不可能有坚固的系统的。只要网络中存在远程控制的渠道,就有可能被黑客利用对整个网络进行破坏。针对网络的攻击,主要的目标集中在网络的接入设备,如拨号服务器、VPN 接入,同时也会针对防火墙等安全防护设备。对于无线接入式的网络,黑客通常尝试对无线信号进行接收,实现对网络中内容的获取。除了达到渗透的目的,攻击者还经常通过拒绝服务的攻击方式对网络进行攻击,阻碍目标网络对外提供正常的服务,从而对企业,尤其是网络服务企业的形象造成极大的影响。

11.4.1 拨号和 VPN 攻击

随着技术的进步,ADSL 等宽带入户的解决方案进入了千家万户。但拨号网络接入以其稳定性和设备的简单性,到现在还被广泛地使用。甚至在一些拥有高速网络接口的企业,由于老设备继续使用、内部办公需要等原因,通常会保留拨号接入的接口。而正是这些接口,可能会对企业网造成可怕的安全影响。对于存在安全保护不当的远程访问服务器的网络,黑客完全可以不必在拥有防火墙保护的接口上费心。通过这些照管不周的接口就可以顺利地实现对网络的入侵。拨号攻击与其他攻击类似,同样要经过踩点、扫描、查点和漏洞发掘 4 个步骤。

拨号攻击的过程主要是利用拨号攻击工具顺序地拨打大量的电话号码,记录有效的数据连接,尝试确认在电话线另一端的系统,再通过猜测,以常用的用户名和保密短语有选择地尝试登录。

1. 准备拨号攻击

拨号攻击首先要确认目标电话号码范围。恶意的黑客通常会从企业名称着手,从能够想到的尽可能多的来源汇集出一个潜在号码范围的清单。这其中最明显的方式是查找电话号码簿。一旦找到企业的主电话号码,入侵者通常会利用自动程序尝试拨打这个端局交换机号码,根据反馈的连接尝试结果获得拨号服务器的号码。

另一个可能的策略是利用社会工程学技术,从安全意识不高的企业人员口中套出目标公司的电话号码信息。这是获得公开的远程访问或数据中心电话线路信息的好方法,通常可以获得与主电话号码不属于同一端局的拨号服务器号码。除了使用电话簿外,目标公司网站也是寻找电话号码的重要信息来源。许多企业会在 Internet 上发布企业完全的电话目录。

除了这些信息以外,对于企业相关人员对外注册信息的搜集更可以进一步获得有用的攻击信息。例如,从网络上公布的域名注册详细信息,攻击者可以获得注册企业的主电

话号码，同时，还可以根据注册人猜测出一个可能的网络用户名称，而通常这个名称的主人属于企业的高层用户或系统的高级管理人员。

除了通过拨号获得拨号服务器可能的号码以外，通过拨号分析，入侵者还可以了解到公司人员的姓名及工作状态信息，包括员工是否在较长时间无法注意到自身用户账号上的异常行为。通过对员工电话问候语的分析，入侵者甚至可以了解到各个人员在企业中的重要程度，并以此进行攻击优先次序的调整。

通过对拨号服务器反馈信息的分析，可以找到易于渗透的调制解调器，在确认这个连接到底有多脆弱时，往往需要仔细检查拨号的信息并手工进行跟踪处理。通过对反馈信息的分析，攻击者可以获得服务器的生产商以及服务器的型号版本，根据这些信息，可以选择正确的登录模式并根据服务器可能的默认账户和存在的漏洞进行进一步的攻击。

2 拨号攻击渗透

当信息搜集有了成果，下一步就是将得到的有价值信息进行分类。通过对服务器连接特性的分析，攻击者构成专门的攻击脚本。利用专门的攻击进行接入性的猜测攻击。影响攻击脚本的因素主要包括：

- 连接是否超时或尝试次数的阈值；
- 超过阈值后的处理措施，如使当前连接无效等；
- 连接是否只在一定时间内允许；
- 认证的方式；
- 用户代号和密码的最大字节数及组成字符的允许范围；
- 是否对 Ctrl+C 等特殊键有反应，从而搜集到额外的信息；
- 系统标示信息，信息是否会出现变化及信息类型。

根据对这些因素相关信息的搜集，就可以对服务器实施攻击渗透。根据以上因素，也可以确认服务器的攻击难度，服务器攻击难度分为以下 5 个级别：

(1) 第 1 级，具有容易猜到的进程使用的密码。

(2) 第 2 级，单一认证，无尝试次数限制。此类系统只有一个密码或 ID，且调制解调器在多次尝试失败后不会断开连接。

(3) 第 3 级，单一认证，有尝试次数限制。此类系统只有一个密码或 ID，但调制解调器在预设的尝试次数失败后会断开连接。

(4) 第 4 级，双重认证，无尝试次数限制。此类系统有两种认证机制。如需要同时确认用户名和密码，调制解调器在多次尝试失败后不会断开连接。

(5) 第 5 级，双重认证，有尝试次数限制。此类系统有两种认证机制。调制解调器在预设的尝试次数失败后会断开连接。

级别越高，攻击的难度越大，脚本的处理也就越敏感。对于属于第 1 级的拨号接入设备，基本上可以通过手工完成猜测过程。根据设备的类型，使用系统默认或其他方式对获得的用户名、密码进行尝试，可以顺利地进入到系统。

对于属于第 2 级的设备，获取访问权所需要的主要是密码。而由于连接尝试没有次

数限制，因此可以通过字典方式的蛮力攻击进行密码猜测。第 3 级的设备与上一级相比攻击的时间相对较多，主要的区别就是在经过一定的猜测尝试后要进行挂起的处理，再重新拨打尝试。对第 4 级和第 5 级的设备的攻击，要输入的信息更多一些，因此其敏感性更高，也更容易犯错。所花的时间也要高出许多。

3. VPN 攻击

由于电话网络的稳定性和普及性，拨号接入在很长一段时间内还会是重要的接入方式。然而技术界不断创新的前沿阵地早已揭示了将来的远程访问机制，那就是 VPN 虚拟专用网。VPN 技术在最近几年蓬勃发展，并稳步进入了公用和私用网络体系。虽然 VPN 相当注重连接的安全性，但在实际生活当中，仍不乏 VPN 网络被成功攻破的事例。

例如，对于微软公司 PPTP 实现，就有着很多的攻击工具。微软公司 PPTP 协议的漏洞主要体现在以下几个方面：

(1) 微软公司的安全认证协议 MS CHAP 依赖于强度很低的传统加密函数 LanManager 散列算法。

(2) 用于加密网络数据的会话密钥的种子数据是根据用户提供的密码生成的，从而潜在地把实际的密钥位长度降到了声明的 40 位或 128 位之下。

(3) 会话加密算法使用对称 RC4 算法，在发送和接收双向会话中密钥被重用，削弱了算法的强度，使得会话容易遭受常见的加密攻击。

(4) 协商和管理连接的控制通道完全未经认证，易遭受拒绝服务型攻击和欺骗攻击。

(5) 只加密了数据有效负载，从而允许窃听者从控制通道分组中获得许多有用的信息。

4. 防范措施

对于拨号攻击的防范主要是对企业中使用的拨号接入设备进行管理，包括对拨号线路进行清点，消除未经授权的拨号连接；同时将拨号服务集中，并隐蔽线路的号码，包括不公开相关的信息，拨号服务号码不在企业公布的电话号码范围以及相关端局范围内；确保拨号设备的物理安全性，提升拨入的认证要求，同时不显示标示信息并对连接操作日志进行定期的分析。当然，除了这些技术上的防范方法，还需要企业在管理上对接入情况有严格的策略，防止接入的随意性和不可控性。

11.4.2　针对防火墙的攻击

现在，防火墙已被公认为企业网络安全防护的基本设备。市场上主要有两类防火墙：应用代理和分组过滤网关。尽管一般认为应用代理比分组过滤网关安全，但应用代理的限制特性和对性能的影响却使得它的适用场合局限于从 Internet 上其他位置外来的分组流动，而不是从企业内部服务器外出的分组流动。而分组过滤网关以及更为先进的全状态分组过滤网关能在许多具有高性能要求的较大机构中较好地运行。

防火墙自开始部署以来，已保护无数的网络躲过恶意的攻击行为，然而它们还远远不是保障网络安全的灵丹妙药。市场上每个防火墙产品几乎每年都有安全脆弱点被发现。更糟糕的是，大多数防火墙往往配置不当，且没有人进行及时的维护和监管，失去了对现

代攻击进行防护的能力。

由于防火墙在开发和使用中存在种种的缺陷,因此攻击者可以利用这些有利的因素,对安置防火墙的企业发动攻击。由于现在的一些错误心理,认为只要安上了防火墙就可以保证企业的安全,攻击者可以轻易地进入到“柔软的网络中心”,进行肆意的破坏而不被及时发觉。

需要指出的是,现实世界中,要想绕过配置得当的防火墙极为困难。然而使用 traceroute,nmap 之类的信息搜集工具,攻击者可以发现或推断出经由目标站点的路由器和防火墙的访问通路,并确定防火墙的类型。当前发现的许多脆弱点,原因在于防火墙的错误配置和缺乏有效的管理维护,这两点一旦被加以利用,所导致的后果将会是毁灭性的。

1. 防火墙的确定

几乎每种防火墙都会发出独特的电子“气味”,即凭借端口扫描、标示获取等方式,攻击者能够有效地确定目标网络上几乎每个防火墙的类型、版本甚至所配置的规则。一旦确认了目标网络的防火墙,攻击者就能够确认防火墙的脆弱点,并利用这些漏洞对目标网络进行渗透。

查找防火墙最简便的方法就是对特定的默认端口执行扫描。市场上一些防火墙使用简单的端口扫描就会显露原形。例如,CheckPoint 的著名防火墙 Firewall 1 监听 256、257 和 258 端口上的 TCP 连接,Microsoft 的 Proxy Server 则通常在 1080 和 1745 端口上监听 TCP 连接。这样,只要利用端口扫描工具对网段中的相关端口进行扫描,就可以轻易确认防火墙的类型。

另一种寻找防火墙的方式是使用 traceroute 这样的路由跟踪工具。检查到达目标主机的路径上每一跳的具体地址和基本名称属性。通常到达目标之前的最后一跳是防火墙的几率很大。当然,如果目标存在不对过期分组进行响应的路由器或防火墙,那么这种寻找很难达到效果,一般需要在获取路径信息后,进行进一步的分析检测,确认最后一跳是否是防火墙。

扫描防火墙有助于寻找防火墙,甚至确认防火墙的类型。但大多数的防火墙并没有打开默认端口进行监听,因此还需要其他一些定位防火墙的方法。与很多的应用服务相类似,许多防火墙在连接的时候都会声明自己的防火墙功能以及类型和版本,这在代理性质的防火墙中更为普遍。通过了解这些标示信息,攻击者就能够发掘出大量已知的漏洞或常见的错误配置。

例如,在 21 号端口上使用 Netcat 连接一台怀疑是防火墙的主机时,可以看到如下的信息:

```
C: \\>nc-v-n 192.168.51.129 21
(UNKNOWN)\[192.168.21.129\] 21 (?) open
220 Secure Gateway FTP server ready
```

其中,Secure Gateway FTP server ready 是老式 Ragle Raptor 防火墙的特征标志。为了进一步确认,连接其 23 号端口:

```
C:\\>nc-v-n 192.168.51.129 23
(UNKNOWN)\[192.168.21.129\] 23 (?) open
Eagle Secure Gateway
Hostname:
```

从以上内容就可以进一步证明该防火墙的类型。同时也可以初步确认，这个防火墙没有经过很严格的安全管理。

如果以上的方法都无法确认防火墙的信息，那么攻击者需要使用很高级的技术查找防火墙的信息。通过探测目标并留意到达目标所经历的路径，攻击者可以推断出防火墙和配置规则。例如，可以用 nmap 工具对目标主机进行扫描，获知哪些端口是打开的，哪些端口是关闭的，以及哪些端口被阻塞。通过对这些信息的分析，可以得到关于防火墙配置的大量素材。

对于一个配置不慎的防火墙来说，攻击者可以通过各种分析和扫描工具检查到它的存在及具体的类型和配置信息。通过这些信息的搜集，攻击者可以查阅手头的资料，找到可以利用的漏洞或逻辑后门透过或绕开防火墙，进入到企业内部。

2 源端口扫描

传统的分组过滤防火墙存在一个很大的缺陷，即不能维持状态信息。由于无法维持状态，防火墙也就不能分辨出连接是源于防火墙外还是内。这样对部分类型的连接就无法有效地控制。例如，对于提供 FTP 服务的网络，为了允许 FTP 数据通道通过防火墙，需要防火墙允许 20 号端口与内部网络高数值端口的连接。这样，如果防火墙不能维护状态信息，就无法追踪一个 TCP 连接与另一个连接的关系，这样，所有从 20 号端口到内部网络高数据端口的连接都允许有效地不加阻挡地通过。

对于这种传统的分组过滤防火墙，可以利用这一弱点攻击防火墙后面脆弱的系统。利用端口重定向工具，可以将远端口设为 20，从而透过防火墙进行漏洞的挖掘工作。

3. 分组过滤防火墙攻击

分组过滤防火墙主要依赖于 ACL 规则确定各个分组是否有权出入内部网络。大多数情况下，这些 ACL 规则是精心设计的，难以绕过。但对于防火墙来说，难免存在不严格的 ACL 规则，允许某些类型的分组不受约束地通过。例如，企业希望自己的 ISP 提供 DNS 服务。相关的规则就可能设为“允许来自 53 号 TCP 源端口的所有活动”，这就是一个很不严格的规则，它将可能允许攻击者从外部扫描整个目标网络。只要攻击者伪装成 53 号端口通信，就可以顺利地透过防火墙进入到企业网络内部，进行扫描和肆意的破坏。

通常，这种规则应设定为“允许来自 ISP 的 DNS 服务器的源和目的 TCP 端口号均为 53 的活动”。这样就可以避免由于允许范围的扩大而造成攻击的可能性。

除了精心定制规则以外，对于部分防火墙，它们都有默认打开的端口。例如，CheckPoint 提供默认打开着的端口，包括 DNS 查找(53 号 UDP 端口)、DNS 区域传送(53 号 TCP 端口)和 RIP(520 号 UDP 端口)。通过这些默认端口的分组数据一般不会进行日志记录。如果攻击者确认了防火墙的类型，就可以用伪装默认端口的方法有效地绕过所设置的防火墙规则。攻击者首先设法在网络内部安装后门程序，这一般可以利用社

会工程学中的种种欺骗手段实现。之后，攻击者就可以利用这些默认的端口与后门程序进行通信，进而在完全没有安全记录的情况下实施对整个内部网络的攻击。

4. 应用代理的攻击

与分组过滤防火墙相比，应用代理的弱点较少。一旦加强了防火墙的安全并实施稳固的代理规则，代理防火墙是难以绕过的。但是，在实际的运行中，对应用代理的错误配置并不少见。

在使用某些较早的 UNIX 代理时，管理员通常会忘记限制本地访问。尽管内部用户访问 Internet 时存在认证要求，但他们却有可能获取到防火墙本身的本地访问权限。如果可以进行本地登录，防火墙本身的安全性就成了更大的问题。以前面在防火墙扫描中提到的 eagle 防火墙为例，在 hostname 中输入 localhost 并使用密码攻击技术，入侵者就有可能获得防火墙的本地访问权限。之后，根据操作系统的弱点进行攻击，入侵者获取 root 用户的权限并进一步控制整个防火墙。

一些应用代理服务器的安全性可能很高，建立了强壮的访问控制规则，但很多时候，系统管理员会忽略禁止外部连接通过该代理的访问权限。由于没有对代理访问进行认证，外部攻击者可能会将这些代理服务器作为发起攻击的跳板，隐藏自己的行踪。

举例来说，对于目前很流行的 WinGate 代理防火墙软件，它的默认参数包含很多的弱点，包括文件认证的 Telnet，SOCKS 和 Web。如果管理员只是简单地安装并且不进行安全性的配置，那么，这个代理软件会被攻击者利用作为攻击的跳板。在网络上，有着大量的诸如此类的代理防火墙，给安全管理员追踪可能的入侵行为带来了很大的困难。对于 WinGate 来说，默认的参数甚至允许用户通过管理端口远程查看系统的文件。这样就给 WinGate 系统本身带来了极大的漏洞，入侵者只需要连接 WinGate 的管理端口，就可以顺利浏览系统中的所有文件，获取系统中存放的用于认证的用户名和密码。

11.4.3　网络拒绝服务攻击

破坏一个网络或系统的运作往往比真正取得它们的访问权限容易得多，现在不断出现的具有强破坏性的种种拒绝服务攻击就说明了这一点。像 TCP/IP 之类的网络互联协议是按照在开放和彼此信任的群体中使用来设计的，在当前的现实环境中却表现出内在的缺陷。此外，许多操作系统和网络设备的网络协议栈也存在缺陷，从而削弱了它们抵抗 DoS 攻击的能力。

DoS 攻击威胁了大范围的网络服务，它不仅造成了服务的中断，部分攻击还会造成系统的完全崩溃甚至设备的损毁，是目前最具有危险性的攻击。

1. DoS 攻击类型

DoS 攻击从攻击目的和手段上主要分为以下一些类型，它们以不同的方式对目标网络造成破坏。

（1）带宽耗用 DoS 攻击

最阴险的 DoS 攻击是带宽耗用攻击。它的本质就是攻击者消耗掉通达某个网络的所有可用的带宽。这种攻击可以发生在局域网上，不过更常见的是攻击者远程消耗资源。

为了达到这一目的，一种方法是攻击者通过使用更多的带宽造成受害者网络的拥塞。对于拥有 100Mbps 带宽网络的攻击者来说，对于 T1 连接的站点进行攻击可以完全填塞目标站点的网络链路。另一种方法是攻击者通过征用多个站点集中拥塞受害者的网络连接来放大 DoS 攻击效果。这样带宽受限的攻击者就能够轻易地汇集相当高的带宽，成功地实现对目标站点的完全堵塞。

（2）资源衰竭 DoS 攻击

资源衰竭攻击与带宽耗用攻击的差异在于前者集中于系统资源而不是网络资源的消耗。一般来说，它涉及诸如 CPU 利用率、内存、文件系统和系统进程总数之类系统资源的消耗。攻击者往往拥有一定数量系统资源的合法访问权。之后，攻击者会滥用这种访问权消耗额外的资源，这样，系统或合法用户被剥夺了原来享有的资源，造成系统崩溃或可利用资源耗尽。

（3）编程缺陷 DoS 攻击

部分 DoS 攻击并不需要发送大量的数据包来进行攻击。编程缺陷攻击就是利用应用程序、操作系统等在处理异常条件时的逻辑错误实施的 DoS 攻击。攻击者通常向目标系统发送精心设计的畸形分组来试图导致服务的失效和系统的崩溃。

（4）基于路由的 DoS 攻击

在基于路由的 DoS 攻击中，攻击者操纵路由表项以拒绝向合法系统或网络提供服务。诸如路由信息协议和边界网关协议之类较早版本的路由协议没有或只有很弱的认证机制。这就给攻击者变换合法路径提供了良好的前提，往往通过假冒源 IP 地址就能创建 DoS 攻击。这种攻击的后果是受害者网络的分组或者经由攻击者的网络路由，或者被路由到不存在的黑洞网络上。

（5）基于 DNS 的 DoS 攻击

基于 DNS 的攻击与基于路由的 DoS 攻击类似。大多数的 DNS 攻击涉及欺骗受害者的域名服务器高速缓存虚假的地址信息。这样，当用户请求某 DNS 服务器执行查找请求的时候，攻击者就达到了把它们重定向到自己喜欢的站点上的效果。

2 DoS 攻击手段

一些 DoS 攻击可以影响许多类型的系统，将系统的网络带宽或资源耗尽。这些攻击的常用要素是协议操纵。如果诸如 ICMP 这样的协议被操纵用于攻击目的，它就有能力同时影响许多系统。DoS 攻击主要有以下攻击手段。

（1）Smurf 攻击

Smurf 攻击是一种最令人害怕的 DoS 攻击。该攻击向一个网络上的多个系统发送定向广播的 ping 请求，这些系统接着对请求做出响应，造成了攻击数据的放大。Smurf 攻击通常需要至少 3 个角色：攻击者、放大网络和受害者。攻击者向放大网络的广播地址发送源地址，伪造成受害者系统的 ICMP 回射请求分组。放大网络中的各个主机相继向受害者系统发出响应。如果攻击者给一个拥有 100 个会对广播 ping 请求做出响应的系统的放大网络发出 ICMP 分组，它的 DoS 攻击效果就放大了 100 倍。这样，大量的 ICMP 分组发送给受害者系统，造成网络带宽的耗尽。

(2) SYN 洪泛

在 Smurf 攻击流行前,SYN 洪泛一度是最具有破坏性的 DoS 攻击。从原理上讲,主要是利用 TCP 连接的三次握手过程中的资源不平衡性。发动 SYN 攻击时,攻击者会发送一个从系统 A 到系统 B 的 SYN 分组,不过他用一个不存在的系统伪装源地址。系统 B 试图发送 SYN/ACK 分组到这个欺骗地址。由于响应的系统并不存在,因此 B 系统就无法收到响应的 RST 分组或 ACK 分组,直到连接超时。由于连接队列的容量通常很小,攻击者通常只需要 10 秒钟发送若干 SYN 分组就能够完全禁止某个特定的端口,造成相对应的服务无法对正常的请求进行响应。这种攻击非常具有破坏性。首先,它成功地引发 SYN 洪泛只需要很小的带宽。其次,由于攻击者对 SYN 分组的源地址进行伪装,而使得 SYN 洪泛成了隐蔽的攻击,查找发起者变得非常困难。

(3) PTR 记录欺诈

递归的功能允许 DNS 服务器处理不是自己所服务区域的解析请求。当某个 DNS 服务器接收到一个不是自己所服务区域的查询请求时,它将把该请求间接传送给所请求区域的权威性 DNS 服务器。从这个权威性服务器接收到响应后,最初的 DNS 服务器把该响应发回给请求方。对于脆弱的 BIND 版本,攻击者利用 DNS 递归的功能,产生虚假的高速缓存 DNS 信息。该攻击称为 PTR 记录欺诈,它发掘的是从 IP 地址映射到主机名称过程中的漏洞。通过将主机名称映射到其他 IP 地址或不存在的 IP 地址,用户就无法正确地获得需要的服务,达到拒绝服务的目的。

3. DDoS 攻击

2000 年 2 月,出现了分布式的拒绝服务攻击,多个著名的网站受到了这种攻击,造成了不可估量的损失。DDoS 攻击的第一步是瞄准并获得尽可能多的系统管理员访问权。这种相当危险的任务通常是用客户化的攻击脚本来指定脆弱的系统。一旦获得了对系统的访问权,攻击者会将 DDoS 软件上传并运行,大多数的 DDoS 服务器程序运行的方式是监听发起攻击的指令。这样攻击者只须将需要的软件上传到尽可能多的受损系统上,然后等待适当的时机发起攻击命令即可。

TFN 攻击是第一个公开的 UNIX 分布式拒绝服务攻击。TFN 有客户端和服务器端组件,允许攻击者将服务器程序安装至远程的系统上,然后在客户端上使用简单的命令,就可以发起完成分布式拒绝服务攻击。

Stacheldraht 更进一步,它将主控与被控之间的通信进行了加密,躲避入侵检测系统的检测。同时它还可以用 rcp 命令在需要时升级服务器组件,进行新的 DDoS 攻击。

11.5　本章小结

黑客攻击的动机主要包括好奇心、个人声望、智力挑战、窃取情报、报复、金钱和政治目的等。

黑客攻击的流程可归纳为踩点、扫描、查点、获取访问权、权限提升、窃取、掩盖踪迹、

创建后门和拒绝服务攻击。

黑客所使用的入侵技术主要包括协议漏洞渗透、密码分析还原、应用漏洞分析与渗透、社会工程学、拒绝服务攻击、病毒或后门攻击。

针对不同的网络有不同的攻击方法，主要的方法有拨号和 VPN 攻击、针对防火墙的攻击、拒绝服务攻击。

习　题

1. 黑客攻击的流程是什么？
2. 黑客是否只有通过计算机才能够获取你的秘密？
3. “会话侦听与劫持技术”属于(　)技术。

   A. 密码分析还原　　B. 协议漏洞渗透

   C. 应用漏洞分析与渗透　　D. DoS 攻击
4. 比较“密码还原技术”和“密码猜测技术”。
5. 拒绝服务攻击的主要目的是什么？
6. 针对防火墙的攻击为什么可能成功？

第12章 漏洞扫描

本章要点：

- 计算机漏洞的定义及存在的原因；
- 网络安全扫描的3个阶段；
- 常用的网络扫描工具；
- 基于网络的扫描和基于主机的扫描的比较。

12.1 计算机漏洞

12.1.1 计算机漏洞的概念

从众多报刊杂志或者网络资源中，人们或许已经对计算机系统的“漏洞”这个概念有了一个感性的理解。确实，这里的“漏洞”并不是一个物理上的概念，它是指计算机系统具有的某种可能被入侵者恶意利用的属性。在计算机安全领域，安全漏洞(security hole)通常又称为脆弱性(vulnerability)。

在研究计算机脆弱性的过程中，对于“计算机脆弱性(computer vulnerability)”这个词组的精确定义争议很大，其中1996年Matt Bishop和Dave Bailey给出的关于“计算机脆弱性”的定义是得到广泛认可的定义之一。

- “计算机系统由一系列描述构成计算机系统的实体的当前配置状态(state)组成，系统通过应用状态变换(state transition)(即改变系统状态)实现计算。使用一组状态变换，从给定的初始状态可以到达的所有状态最终分为由安全策略定义的两类状态：已授权的(authorized)和未授权的(unauthorized)。”
- “脆弱(vulnerable)状态是指能够使用已授权的状态变换到达未授权状态的已授权状态。受损(compromised)状态是指通过上述方法到达的状态。攻击(attack)是指以受损状态结束的已授权状态变换的顺序。由定义可知，攻击开始于脆弱状态。”
- “脆弱性是指脆弱状态区别于非脆弱状态的特征。广义地讲，脆弱性可以是很多脆弱状态的特征；狭义地讲，脆弱性可以只是一个脆弱状态的特征。”

简单地说，计算机漏洞是系统的一组特性，恶意的主体(攻击者或者攻击程序)能够利用这组特性，通过已授权的手段和方式获取对资源的未授权访问，或者对系统造成损害。这里的漏洞既包括单个计算机系统的脆弱性，也包括计算机网络系统的漏洞。当系统的某个漏洞被入侵者渗透(exploit)而造成泄密时，其结果就称为一次安全事件(security

incident)。

12.1.2　存在漏洞的原因

现在仍然在 Internet 上使用的基础协议中,有很多早期的协议在最初设计时并没有考虑安全方面的需求。另外,无论从物理的拓扑连接还是应用于其上的技术来看,Internet 都是一个变化相当迅速的动态环境。要在这样一个基础并不安全的、动态的、分布的环境中保证应用的安全就变得比较困难。

正是由于 Internet 的开放性和 Internet 协议的原始设计,在 Internet 上实施普通的电子攻击可以是快速、容易、低成本的,甚至有些攻击很难被检测或者跟踪到。攻击者无须与被攻击的目标有物理上的接触,就可以通过无所不在的网线将他实施攻击的电子信号传递到四面八方,而他自己却可以隐藏在世界上任何一个不为人知的地点。他甚至可以"攻破"(取得特殊权限)某一个站点将其作为自己的据点。

即便如此,很多站点仍然在 Internet 上使用没有安全保证的信任策略。也有很多站点甚至连他们在 Internet 上使用的是什么信任策略都不清楚。这些站点可能认为攻击者不会将自己作为目标,或者认为自己已经对可能的攻击做好足够的预防。但 Internet 上应用的技术可以说是瞬息万变的,攻击者的技术和工具也在不断发展,任何一种安全的解决方案都必须不断更新才能够适应这样的变化。

另外,在 Internet 上传送的很多数据都是没有加密的明文,这不仅威胁到使用明文传输的各种应用,也威胁到某些认证和授权的方式。因为明文传输使得嗅探(sniffer)网络数据成为可能。如果某一个站点被安装了网络嗅探软件,且这个站点允许入侵者嗅探其他区域的网络数据,它就很可能威胁到其他站点的安全性。

Internet 上存在漏洞的另一个原因是 Internet 上高速膨胀的应用类型。各种各样崭新的、复杂的网络服务软件层出不穷,通常这些服务在设计、部署和维护阶段都会出现安全问题。在将新产品快速推入市场的过程中,程序员不能保证他们不犯以前犯过的错误,也不能保证不引入新的错误,这都可能造成服务软件本身的漏洞。另一方面,一些商业操作系统通常宣称自己为迎合用户的需求而设计,为了提供易用性、易维护性而牺牲一些安全性。虽然在很多时候用户都可以通过自定义安全策略加强安全性,但事实上很少有用户会这么做。另外,快速增加的复杂应用需要大量经过培训的系统管理员或者专家用户,而实际的情况是很多没有经验的管理员被委以安全管理的任务。这些情况都增加了系统被攻击的机会。

从技术角度而言,漏洞的来源主要有以下几个方面:

(1) 软件或协议设计时的瑕疵

协议定义了网络上计算机会话和通信的规则,如果在协议设计时存在瑕疵,那么无论实现该协议的方法多么完美,它都存在漏洞。网络文件系统(network file system,NFS)便是一个例子。NFS 提供的功能是在网络上共享文件,这个协议本身不包括认证机制,也就是说无法确定登录到服务器的用户确实是某一个用户,所以 NFS 经常成为攻击者的目标。另外,在软件设计之初,通常不会存在不安全的因素。然而当各种组件不断添加进来的时候,软件可能就不会像当初期望的那样工作,从而可能引入不可知的漏洞。

（2）软件或协议实现中的弱点

即使协议设计得很完美，实现协议的方式仍然可能引入漏洞。例如，和 E-mail 有关的某个协议的某种实现方式能够让攻击者通过与受害主机的邮件端口建立连接，达到欺骗受害主机执行意想不到的任务的目的。如果入侵者在“To:”字段填写的不是正确的 E-mail 地址，而是一段特殊的数据，受害主机就有可能把用户和密码信息送给入侵者，或者使入侵者具有访问受保护文件和执行服务器上程序的权限。这样的漏洞使攻击者不需要访问主机的凭证就能够从远端攻击服务器。

（3）软件本身的瑕疵

这类漏洞又可以分为很多子类。例如，没有进行数据内容和大小检查，没有进行成功/失败检查，不能正常处理资源耗尽的情况，对运行环境没有做完整检查，不正确地使用系统调用，或者重用某个组件时没有考虑到它的应用条件。攻击者通过渗透这些漏洞，即使不具有特权账号，也可能获得额外的、未授权的访问。

（4）系统和网络的错误配置

这一类的漏洞并不是由协议或软件本身的问题造成的，而是由服务和软件的不正确部署和配置造成的。通常这些软件安装时都会有一个默认配置，如果管理员不更改这些配置，服务器仍然能够提供正常的服务，但是入侵者就能够利用这些配置对服务器造成威胁。例如，SQL Server 的默认安装就具有用户名为 sa、密码为空的管理员账号，这确实是一件十分危险的事情。另外，对 FTP 服务器的匿名账号也同样应该注意权限的管理。

12.1.3 公开的计算机漏洞信息

计算机系统的漏洞本身不会对系统造成损坏。漏洞的存在，只是为入侵者侵入系统提供了可能。正因为如此，早期的很多人都认为应该把发现的漏洞隐瞒起来，至少不应该让每一个 Internet 用户都知晓。这样知道漏洞的人越少，系统就越安全。但事实上真正的入侵者总是有办法从各种渠道获得各种漏洞的相关信息，他们也能够使用各种方法找出网络上存在漏洞的系统。因此，漏洞的公开，受益最大的还是系统管理员。公开漏洞可以促使提供软件或硬件的厂商更快地解决问题，也可以让系统管理员更有针对性地对自己管理的系统进行配置和管理。多年的实践也使人们逐渐认识到，建立在漏洞公开基础之上的安全才是更可靠的安全。Internet 上已经有许多关于各种漏洞的描述和与此相关的数据库。下面是一些比较权威的漏洞信息资源。

1. 通用漏洞和曝光

通用漏洞和曝光（CVE）是一个公共安全漏洞和曝光信息的标准化名字列表。它致力于为所有公开的漏洞和安全曝光名称标准化的工作。CVE 是一个字典而不是数据库，它的目标是使不同的漏洞数据库共享数据和搜索信息变得更加容易。目前已经有 200 多个组织、产品和安全警告提供服务实现了“CVE 兼容”。更加具体的信息可以访问 CVE 的网站 www.cve.mitre.org。

2. BugTraq 漏洞数据库

BugTraq 是由 SecurityFocus 公司维护的一个关于计算机安全漏洞详细信息讨论的

邮件列表,讨论内容包括漏洞的描述、漏洞的渗透方法及漏洞的修补方法等。与这个邮件列表相关的漏洞数据库是一个 CVE 兼容的数据库,提供了包括以上讨论内容在内的非常详细的漏洞信息。任何人都可以从 Internet 上检索这个数据库,而且该数据库提供了 5 种检索方式:软件提供商、标题、关键字、BugTraq ID 和 CVE ID。另外需要提及的是,BugTraq 漏洞数据库包括的某些漏洞并没有 CVE ID,所以有的安全工具的漏洞库里既提供 CVE ID,也提供 BugTraq ID,以方便用户检索漏洞信息。

3. ICAT 漏洞数据库

ICAT 是由美国标准技术研究所(National Institute of Standard Technology,NIST)维护的一个 CVE 兼容的漏洞信息检索索引。它提供了非常灵活的检索方式,任何人都可以从 Web 页面进行检索,同时 ICAT 也提供可以下载的 Microsoft Access 格式的数据库文件。每条漏洞记录的信息包括漏洞的 CVE 名字、发布时间、描述、危险等级、漏洞类型、实施范围、受影响系统和参考链接等。

4. CERT/CC 漏洞信息数据库

CERT/CC 漏洞数据库也是一个 CVE 兼容的数据库。可以通过名字、ID 号、CVE 名字、公布日期、更新日期和严重性等方法检索漏洞信息。漏洞记录包括漏洞描述、影响、解决方案、受影响系统和参考链接等信息。

5. X-Force 数据库

X-Force 数据库由 ISS 公司维护,是一个比较全面的漏洞信息数据库。可以在 Web 页面上使用关键字对数据库进行检索,检索到的漏洞记录包括漏洞描述、受影响平台、补救措施、风险等级、影响结果、报告时间和参考链接等信息。与上面几个数据库一样,它也是 CVE 兼容的。

12.2 实施网络扫描

黑客在真正侵入系统之前,通常都会先进行下面 3 项工作:踩点、扫描和查点。

一次完整的网络扫描主要分为以下 3 个阶段:

(1) 发现目标主机或网络。

(2) 发现目标后进一步搜集目标信息,包括操作系统类型、运行的服务及服务软件的版本等。如果目标是一个网络,还可以进一步发现该网络的拓扑结构、路由设备及各主机的信息。

(3) 根据搜集到的信息判断或者进一步检测系统是否存在安全漏洞。下面将分别说明这 3 个阶段使用的扫描技术和方法。

12.2.1 发现目标

这一阶段就是通过发送不同类型的 ICMP 或者 TCP,UDP 请求,从多个方面检测目标主机是否存活。在这一阶段使用的技术通常称为 ping 扫射(ping sweep),包括 ICMP

扫射、广播 ICMP、非回显 ICMP、TCP 扫射、UDP 扫射。

1. ICMP 扫射

ICMP 是 IP 层的一个组成部分，用来传递差错报文和其他需要注意的信息。经常用到的 ping 命令就是使用的 ICMP。ICMP 报文是在 IP 数据报内部传输的，如图 12-1 所示。ICMP 的正式规范参见 RFC792。

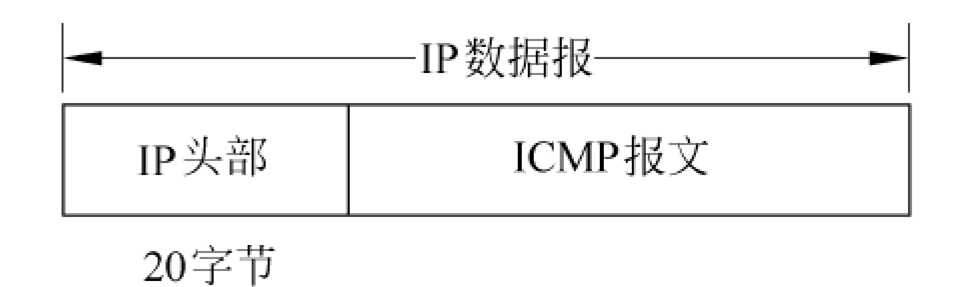


图 12-1　ICMP 报文封装在 IP 数据报内

ICMP 报文的格式如图 12-2 所示。报文的前两个字节决定了报文的类型。第 3 个和第 4 个字节是 ICMP 报文的校验和字段。

ICMP 扫射利用了类型为 8 的 ICMP 报文，即 ICMP 回显请求。通常网络上收到 ICMP 回显请求的主机都会向请求者发送 ICMP 回显应答(类型为 0)报文。这样，如果发送者接收到来自目标的 ICMP 回显应答，就能知道目标目前处于存活状态；否则可以初步判断主机没有在线。使用这种方法轮询多个主机称为 ICMP 扫射。这是用来发现目标的最原始的方法。

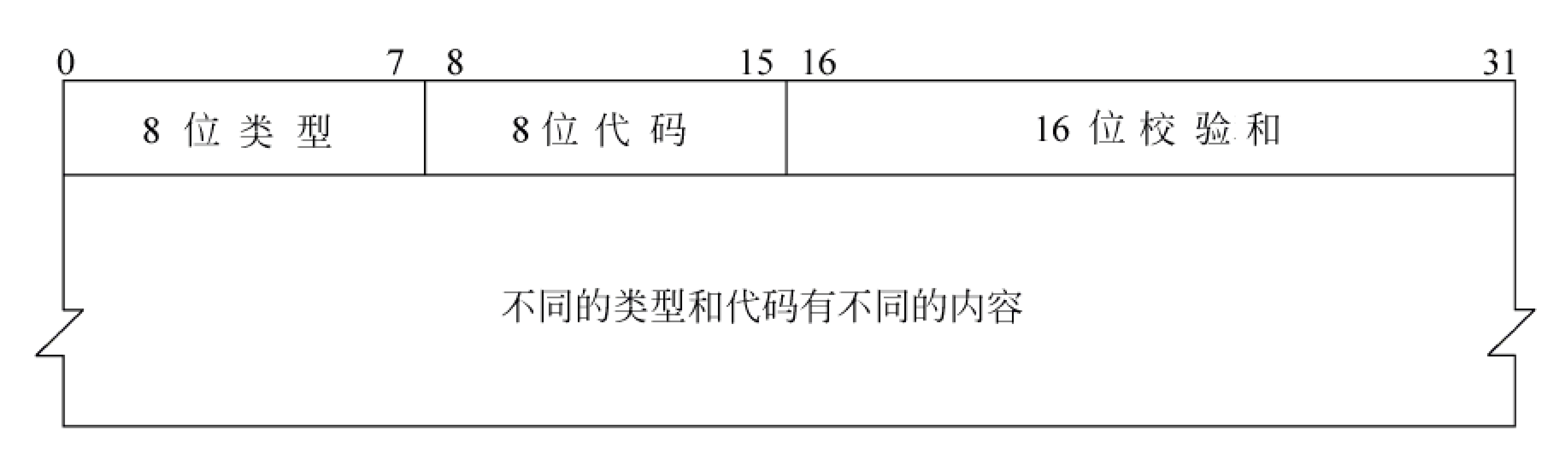


图 12-2　ICMP 报文格式

可用于 ICMP 扫射的工具很多。在 UNIX 环境中主要有 ping 和 fping。传统的 ping 在执行扫射时速度很慢，因为它在探测下一台潜在主机前要等待当前探测的系统给出响应或者超时。而 fping 在扫射多个 IP 地址时，速度明显超过 ping 的速度。与 fping 一同使用的有一个叫作 gping 的工具，它为 fping 生成扫射的 IP 地址列表。在 Windows 环境中可以使用出自 Rhino9 的 Pinger。另外，nmap 的 SP 选项也提供了 ICMP 扫射的能力。

ICMP 扫射虽然非常简单，但它并不十分可靠。因为目标可以阻止对 ICMP 回显请求做出应答。

2. 广播 ICMP

与 ICMP 扫射一样，广播 ICMP 也是利用了 ICMP 回显请求和 ICMP 回显应答这两种报文。但是不同之处在于，广播 ICMP 只需要向目标网络的网络地址和/或广播地址发送一两个回显请求，就能够收到目标网络中所有存活主机的 ICMP 回显应答。因此这样比使用 ICMP 回显请求去轮询目标网络中的主机更加简便。然而这种技巧的一个限制使得它并不像看上去那么诱人。那就是只有 UNIX 系统的主机会对目标地址为网络地址或者广播地址的 ICMP 回显请求做出应答，而 Windows 系统的主机会将其忽略。

例如，在网络 192.168.1.0/24 中有 4 台活动的主机，其中 192.168.1.1 和 192.168.1.2

运行的是 Linux 操作系统，而 192.168.1.3 和 192.168.1.4 运行的是 Windows 操作系统。那么如果在 192.168.1.1 上执行目标地址为广播地址的 ping 命令，则会得到下面的结果：

```
\[root@ localhost root\]# ping 192.168.1.0-b
WARNING: pinging broadcast address
PING 192.168.1.0 (192.168.1.0) from 192.168.1.1 : 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq= 1 ttl= 255 time= 0.362 ms
64 bytes from 192.168.1.2: icmp_seq= 2 ttl= 255 time= 0.565 ms
64 bytes from 192.168.1.1: icmp_seq= 3 ttl= 255 time= 0.164 ms (dup!)
64 bytes from 192.168.1.2: icmp_seq= 4 ttl= 255 time= 0.246 ms (dup!)
…
```

另外，如果在一个数量庞大的 UNIX 主机构成的网络上采用此种技巧，可能会同时收到大量的应答，从而造成扫描者的 DoS。

3. 非回显 ICMP

如果目标主机阻塞了 ICMP 回显请求报文，仍然可以通过使用其他类型的 ICMP 报文探测目标主机是否存活。例如类型为 13 的 ICMP 报文(时间戳请求)和类型为 17 的 ICMP 报文(地址掩码请求)。ICMP 时间戳请求允许系统向另一个系统查询当前的时间。ICMP 地址掩码请求用于无盘系统引导过程中获得自己的子网掩码。下面的例子使用一个叫做 icmpenum 的工具对目标进行 ICMP 时间戳请求探测。

```
\[root@ localhost root\]# icmpenum-i2-c 192.168.1.0
192.168.1.1 is up
192.168.1.2 is up
192.168.1.3 is up
192.168.1.4 is up
```

对于 ICMP 地址掩码请求报文而言，虽然 RFC1122 规定，除非是地址掩码的授权代理；否则一个系统不能发送地址掩码应答(为了成为授权代理，必须进行特殊配置)。但是大多数主机在收到请求时都会发送一个应答，甚至有些主机还会发送差错的应答。所以也可以使用类型为 17 的 ICMP 报文来探测主机是否存活。

4. TCP 扫射

传输控制协议(transmission control protocol，TCP)为应用层提供一种面向连接的、可靠的字节流服务。它使用“3 次握手”的方式建立连接。和 ICMP 报文一样，TCP 报文也封装在一个 IP 数据报中，如图 12-3 所示。TCP 的正式规范参见 RFC793。

从建立连接的过程可以知道，如果向目标发送一个 SYN 报文，则无论是收到一个 SYN/ACK 报文还是一个 RST 报文，都表明目标处于存活状态。这就是 TCP 扫描的基本原理。与此类似，也可以向目标发送一个 ACK 报文，按照 RFC793 的规定，如果目标存活，则会收到一个 RST 报文。

TCP 扫射看起来比利用 ICMP 协议进行探测更加有效，事实也正是如此。但 TCP

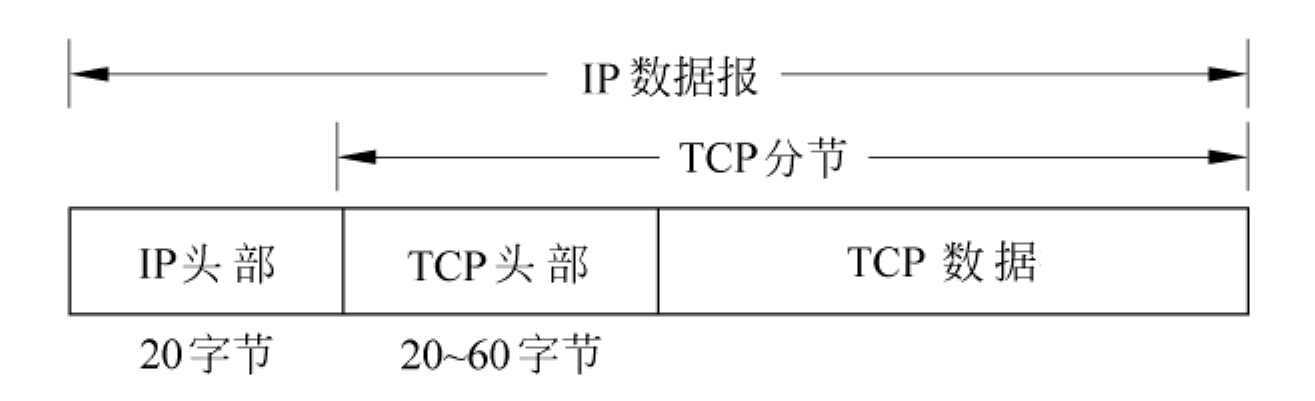


图 12-3　TCP 报文封装在 IP 数据报中

扫射也不是百分之百可靠,因为有的防火墙能够伪造 RST 报文,从而造成防火墙后的某个主机存活的假象。

5. UDP 扫射

用户数据报协议(user datagram protocol, UDP)是一个面向数据报的传输层协议。UDP 数据报也封装在 IP 数据报之中,如图 12-4 所示。RFC768 是 UDP 协议的正式规范。

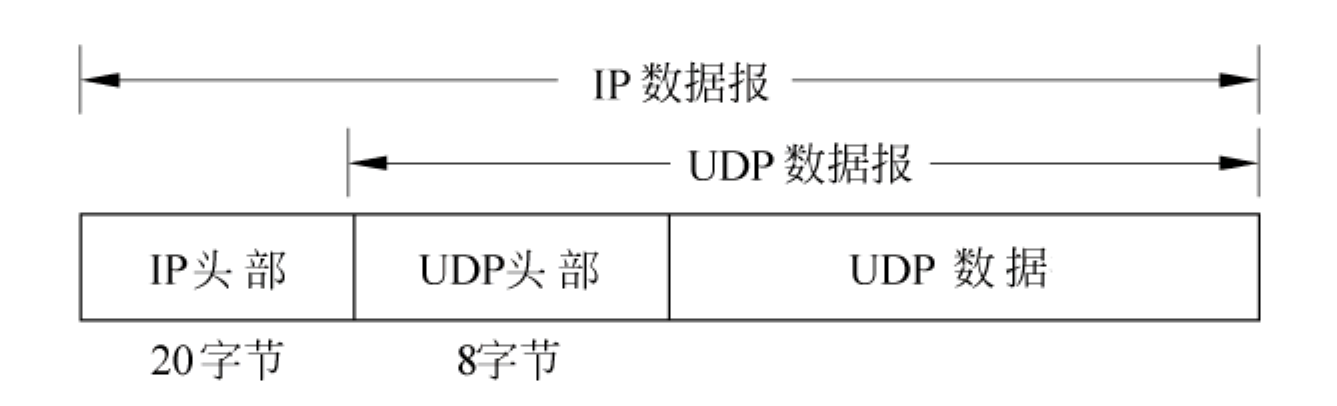


图 12-4　UDP 数据报封装在 IP 数据报中

UDP 协议的规则之一是如果接收到一份目的端口并没有处于侦听状态的数据报,则发送一个 ICMP 端口不可到达报文;否则不做任何响应。这样,如果向目标的特定端口发送一个 UDP 数据报之后,接收到 ICMP 端口不可到达的错误,则表明目标处于存活状态;否则表明目标不在线或者目标的相应 UDP 端口是打开的。由于 UDP 和 ICMP 错误都不保证能到达,因此在一个数据报看上去丢失的时候,还应该重新发送新的 UDP 数据报以确认目标没有发送错误消息。这种方法很不可靠,因为路由器和防火墙都有可能丢弃 UDP 数据报。另外,逐一扫描 UDP 端口通常是很慢的,因为 RFC1812 的 4.3.2.8 节对路由器产生 ICMP 错误消息的速率做了规定(Windows 系统并没有遵守 RFC 的规定,因此对 Windows 系统例外)。例如,Linux 的内核(在 net/ipv4/icmp. h 中)限制产生目的不可到达消息的速率是每 4 秒 80 次,如果超过上限则再增加 1/4 秒的延迟。Solaris 有着更严格的限制(大约每秒两次就会延迟),所以这要耗费相当长的时间。UDP 扫描也有一个好处,就是它可以使用 IP 广播地址,如果向广播地址的高端端口发送一个 UDP 数据报,在没有防火墙过滤的情况下,将收到很多来自目标网络的 ICMP 端口不可到达的错误消息。当然,这也可能造成扫描者自己的 DoS。

表 12-1 对上面 5 种发现目标的技巧做了一个简单的比较。

表 12-1　目标发现阶段的 5 种技巧

名　称	方　法	优　　点	缺　　点
ICMP 扫射	使用 ICMP 回显请求轮询目标主机	使用简单	速度较慢 如果目标关闭了对 ICMP 回显请求的响应，就不能被发现
广播 ICMP	发送 ICMP 回显请求到目标网络的网络地址或广播地址	使用简单，速度比 ICMP 扫射快	不能发现 Windows 主机 如果目标关闭了对 ICMP 回显请求的响应，就不能被发现 可能造成扫描者的 DoS
非回显 ICMP	发送其他类型的 ICMP 报文到目标主机	不受目标阻止 ICMP 回显请求的影响	根据 RFC 的规定和不同操作系统的具体实现，某些类型的 ICMP 请求在探测目标时会受到限制
TCP 扫射	发送 TCP SYN 或者 TCP ACK 到目标主机	最有效的目标发现方法	对入侵者而言，防火墙可能影响这种方法的可靠性
UDP 扫射	发送 UDP 数据报到目标网络广播地址或主机	不受目标阻止 ICMP 回显请求的影响 类似广播 ICMP 可以发送到目标网络广播地址	可靠性低 对于非 Windows 的目标主机，速度慢

1222　攫取信息

广义地讲，在入侵系统之前所做的一切工作都可以称为信息攫取，包括踩点、扫描和查点。因为这些工作总是在搜索着这样或者那样的信息。这一节要讲的主要是扫描阶段信息攫取的技术和方法。

在找出网络上存活的系统之后，下一步就是要得到目标主机的操作系统信息和开放的服务信息。用到的技术主要有端口扫描(port scanning)、服务识别和操作系统探测(operating system detection)。

1. 端口扫描

端口扫描是要取得目标主机开放的端口和服务信息，从而为下一步的“漏洞检测”做准备。根据 RFC1700 规定的已分配端口，网络服务和端口是一一对应的。如 FTP 服务通常开设在 TCP 21 端口，TELNET 服务通常开设在 TCP 23 端口。进行端口扫描，可以快速获得目标主机开设的服务。下面分别说明常用的端口扫描类型。

(1) TCP connect( )扫描

端口扫描最基本的方法就是 TCP connect( )扫描。它利用操作系统提供的 connect( )系统调用，与每一个感兴趣的目标计算机的端口进行连接。如果目标端口处于侦听状态，那么 connect( )就能成功；否则，该端口是不能用的，即没有提供服务。这种方法具有以下优点：

- 不需要任何特殊权限，系统中的任何用户都有权利使用这个调用；

- 可以同时打开多个套接字，从而加速扫描，使用非阻塞 I/O 还允许设置一个低的时间用尽周期，同时观察多个套接字。

这种方法对于入侵者而言具有明显的缺点，即容易被过滤或记录。而对于安全管理员而言，使用这种方法的唯一缺点是速度较慢。

(2) TCP SYN 扫描

在前面介绍 TCP 扫射时曾解释了建立 TCP 连接的“3 次握手”过程。当时只是说如果向目标特定端口发送一个 SYN 报文，只要接收到来自目标的响应就表明目标处于存活状态。但可以很容易看出，只要再辨别一下接收到的响应是 SYN/ACK 报文还是 RST 报文，就能够知道目标的相应端口是出于侦听状态还是关闭状态。这就是 TCP SYN 扫描的原理。TCP SYN 扫描又叫“半开扫描”，因为它只完成了 3 次握手过程的一半。

(3) TCP ACK 扫描

TCP ACK 扫描不是用于确定目标打开了哪些端口，而是用来探测防火墙的规则设计。可以确定防火墙是简单的包过滤还是状态检测机制。

(4) TCP FIN 扫描

根据 RFC793 的规定，如果处于侦听状态的端口接收到一个 FIN 报文，则不做任何回应；如果处于关闭状态的端口接收到一个 FIN 报文，则响应一个 RST 报文。据此，可以用 FIN 报文来探测目标打开了哪些端口。然而事实上有一些操作系统(特别是 Windows 系统)，无论端口是打开还是关闭都会响应一个 RST 报文，所以 FIN 扫描通常只工作在基于 UNIX 的 TCP/IP 协议栈上。

(5) TCP XMAS 扫描

向目标发送一个 URG/PSH/FIN 报文，根据 RFC793 的规定，如果目标相应端口打开，则不会收到来自目标的任何回应；否则会收到一个 RST 报文。

(6) TCP 空扫描

向目标发送一个所有标记位都置 0 的报文，根据 RFC793 的规定，如果目标相应端口打开，则不会收到来自目标的任何回应；否则会收到一个 RST 报文。

(7) FTP 反弹扫描

FTP 协议的一个特点是它支持代理 FTP 连接。即入侵者可以将自己的计算机和目标主机的 FTP 服务器建立一个控制通信连接。然后，请求这个服务器激活一个有效的数据传输进程来给 Internet 上的任何地方发送文件。尽管 RFC 明确地定义请求一个服务器发送文件到另一个服务器是可以的，但现在很多 FTP 服务器都不支持这一功能了，或者允许用户禁止此项功能。因为利用这一功能可以通过 FTP 服务器对其他主机进行端口扫描，即使这些主机对入侵者而言是在防火墙后面。

下面是使用这一技术进行端口扫描的一个例子。入侵者首先连接到 192.168.1.1 的 FTP 服务器上，然后使用 PORT 命令来表示被动的用户数据传输进程正在目标计算机上的某个端口侦听，接着入侵者试图用 LIST 命令列出当前目录，其结果通过服务器数据传输进程发送出去。如果目标主机正在某个端口侦听，传输就会成功；否则会出现拒绝连接

的错误。在例子中，目标计算机(192.168.1.3)的 21 端口是打开的，而 22 端口是关闭的。这种方法的优点是难以跟踪，能穿过防火墙。主要缺点是速度很慢，另外有的 FTP 服务会关闭代理功能。

```
220-Serv-U FTP Server ready...
USER anonymous
331 User name okay,need password.
PASS guest@ unknown.com
230 User logged in,proceed.
PORT 192,168,1,3,0,21
200 PORT Command successful.
LIST
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
PORT 192,168,1,3,0,22
200 PORT Command successful.
LIST
150 Opening ASCII mode data connection for /bin/ls.
426 Data connection closed,transfer aborted.
```

(8) UDP 扫描

UDP 扫描和前面的 UDP 扫射的原理完全一样。在这里只是强调它的另一个作用，即发现目标打开的 UDP 端口。

2 服务识别

前面提到，端口扫描的主要目的是为了获得目标主机提供的服务，而通常获取服务类型的办法是根据 RFC1700 直接推断。但是下面几种情况可能会使这项工作变得稍微有些麻烦：

- 该主机将某服务故意开设到了非标准端口；
- 该主机开设了一个 RFC1700 中未定义的服务；
- 该主机被安置了后门程序。

所以有时候仅凭端口号来判断服务类型还是不够的，可能需要更多的信息。下面有一个最简单的例子，扫描发现目标主机 192.168.1.1 的 12345 号 TCP 端口是打开的，在 RFC1700 中没有定义此端口对应的服务，首先可以使用 Netcat 尝试与目标的该端口建立连接，根据返回的信息做出初步判断，在此例中很容易地知道对方运行的服务是 IIS 的 FTP 服务。

```
C:\\>nc 192.168.1.1 12345
220 Microsoft FTP Service
```

像上面例子中那样主动提供旗标信息或者握手信息的服务不妨将其称为主动式服务器。另外还有一类服务需要客户端首先发送一个命令，然后再做出响应。要判断这样的服务，必须首先猜测服务类型，然后模仿客户端发送命令，等待服务器的回应。下面便是

一个这样的例子。当然,这一次我们非常幸运,第一次就猜中了对方运行的是 IIS 5.1 的 WWW 服务。

```
C:\\>nc 192.168.1.1 12346
HEAD/HTTP/1.0
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Content-Location: http: //192.168.1.1: 12346/index.htm
Date: Fri,02 May 2003 11:56:03 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed,08 Jan 2003 09:02:34 GMT
ETag:"30ba3caff4b6c21:86c"
Content-Length: 516
```

这样,如果要让一个工具能够判断任意端口的任意服务类型,或者至少能够判断任意端口的常见服务类型,实现的方法之一就是建立服务特征数据库,服务特征包括服务器软件旗标信息、服务器软件握手信息、服务器软件对特定命令的回应等。检测服务的过程实际上就是模仿客户端软件与服务器软件建立连接并通信。由于服务器软件都具有唯一的特征供客户端软件进行识别,所以识别任意一种服务的通常步骤应该如图 12-5 所示。

只要数据库中含有相应服务器软件的资料,并且能保证该资料是服务器软件的唯一特性,那么识别任意端口的已知服务都是可以实现的。

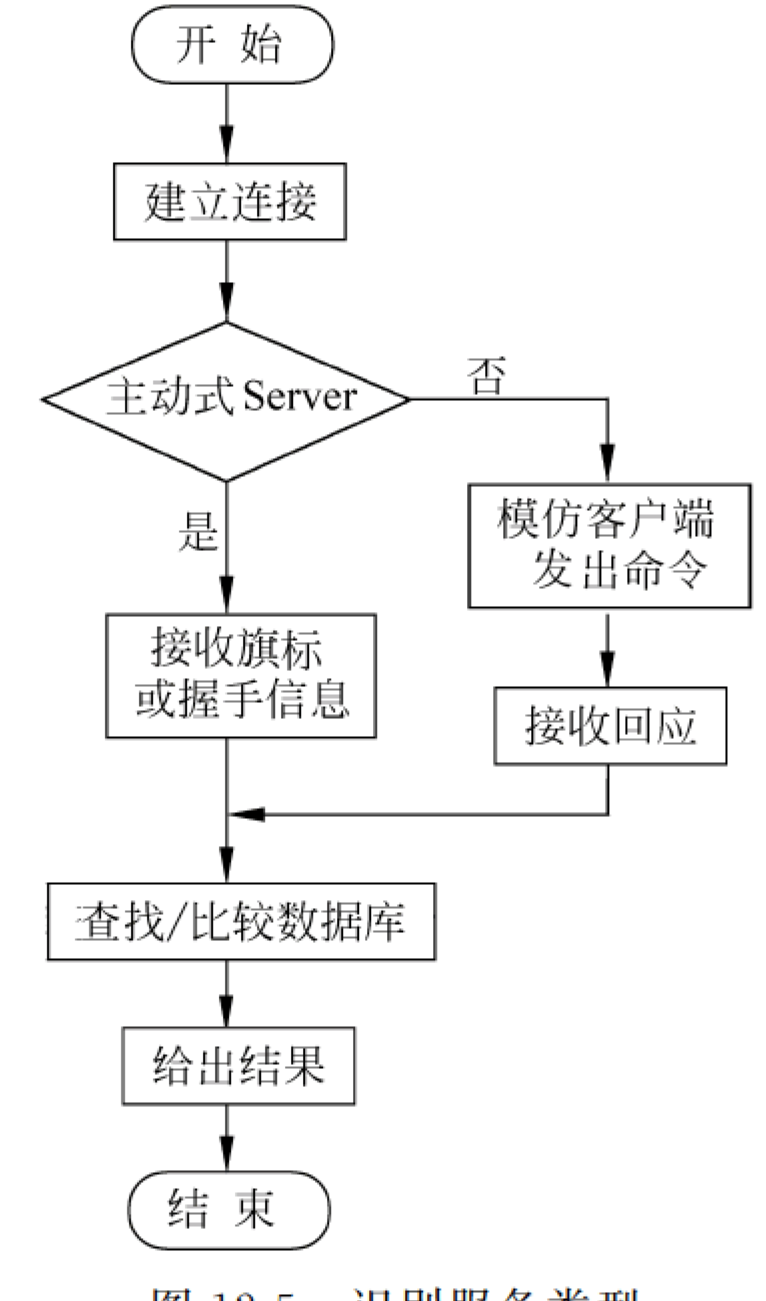


图 12-5　识别服务类型

3. 操作系统探测

由于许多漏洞是和操作系统紧密相关的,因此,确定操作系统类型对于脆弱性评估工具而言也十分重要。目前用于探测操作系统的方法主要可以分为两类:利用系统旗标信息和利用 TCP/IP 堆栈指纹。而后者又有多种不同的实现方法。

利用系统旗标信息是最原始的探测方法。然而它至今仍然被包括 ISS 在内的许多网络安全扫描工具使用,因为在大多数情况下,操作系统的多种服务都会暴露其“身份”,例如 Telnet,WWW,FTP 和 SMTP 等。同时,这种方法实现起来也特别简单。但是在很多情况下,管理员出于安全考虑都会修改或者关闭旗标信息,或者目标机器并不提供有旗标信息的服务,在这样的情况下,这种方法就不能发挥作用了。

利用 TCP/IP 堆栈指纹识别操作系统是近年来发展迅速的一类技术。这类技术的出现主要基于以下几个原因:每个操作系统通常都使用自己的 IP 栈实现;TCP/IP 规范并

不是被严格地执行，每个不同的实现将会拥有自己的特点；规范中一些选择性的特性可能在某些系统中使用，而在其他系统中则没有使用；某些系统私自对 IP 协议做了改进。

目前主要的网络堆栈特征探测技术有如下几种：ICMP 响应分析、TCP 报文响应分析、TCP 报文延时分析和被动特征探测。

(1) ICMP 响应分析

这种方法向目标发送 UDP 或者 ICMP 报文，然后分析目标响应的 ICMP 报文的内容，根据不同的响应特征来判断操作系统。前面已经介绍过，ICMP 数据报是封装在 IP 数据报之内的，而且这种判断操作系统的方法也利用了 IP 头部的字段内容，所以在具体说明这种方法使用的技术之前，有必要先熟悉一下 IP 数据报的头部。其中需要注意的是服务级别 TOS、总长度、标识、DF 位、生存期 TTL 和校验和字段。

下面分别说明 ICMP 响应分析方法使用的具体技术。

① ICMP 差错报文引用大小。ICMP 的规则之一是 ICMP 差错报文必须包括生成该差错报文的数据报 IP 头部(包含任何选项)，还必须至少包括跟在该 IP 头部后面的前 8 个字节。图 12-6 显示了由 UDP 数据报引起的 ICMP 端口不可到达差错报文。

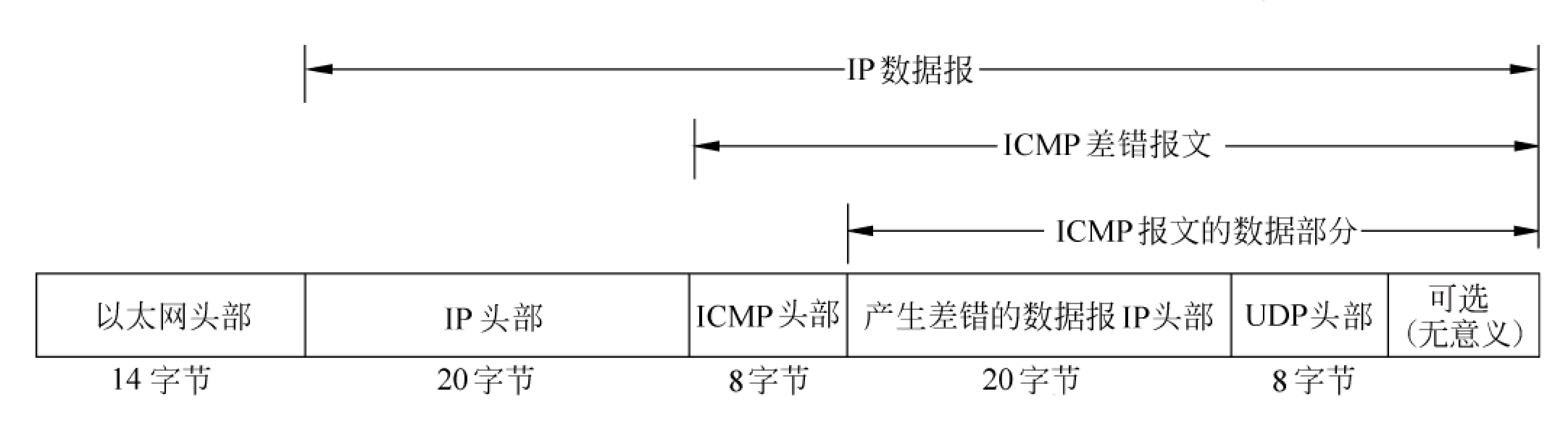


图 12-6　“UDP 端口不可到达”差错报文

导致差错的数据报中的 IP 头部要被送回的原因是 IP 头部中包含了协议字段，使得 ICMP 可以知道如何解释后面的 8 个字节(在图 12-6 中是 UDP 头部)。

大多数操作系统都只返回产生差错的数据报的 IP 头部后的前 8 个字节，然而有一些操作系统在这 8 个字节之后还返回更多的字节(这些字节通常是没有任何意义的)。这样的系统包括 Linux(内核 2.0.x/2.2.x/2.4.x)、SUN Solaris、HPUX 11.x、MacOS 7.55/8.x/9.04、Nokia 系统、Foundry 交换机和其他一些操作系统或者网络设备。

② ICMP 差错报文回显完整性。

一般而言，在发送 ICMP 差错报文时，差错报文的数据部分，只有产生差错的数据报 IP 头部的 TTL 字段和 IP 头部校验和字段会与初始报文不同，因为初始报文到达目标之前会经过一系列的路由设备，而每经过一个设备 TTL 都会减一，相应的校验和也要重新计算。然而实际情况是，有些操作系统会改变产生差错的数据报 IP 头部的其他字段的内容和/或后面数据的内容。如果用 UDP 数据报产生的端口不可到达差错报文来进行分析，可以利用的特点包括下面一些内容：

- IP 数据报总长度 AIX 4.x 和 BSDI 4.1 等操作系统的 IP 栈会将产生差错的数据报 IP 头部的总长度字段加上 20，而另一些系统会将这个字段的数值减少 20，更多的系统会保持这个字段的内容不变。

• IP 数据报标识(IPID)。

FreeBSD 4.0,OpenVMSs 和 ULTRIX 等系统的 IP 栈不能正确回显产生差错数据报的 IPID,它们回显的 IPID 的位顺序和初始顺序不同。其他更多的系统则能够正确回显 IPID 字段。

• 分段标志(3 位)和片偏移。

有一些系统会改变产生差错的数据报头部中 3 位分段标志和片偏移字段的位顺序,而另一些系统只能正确回显。

• IP 头部校验和。

FreeBSD 4.0,OpenVMSs 和 ULTRIX 等系统会将产生差错的数据报 IP 头部的校验和字段置为 0,而大多数的系统只是将重新计算的校验和回显。

• UDP 头部校验和。

FreeBSD 4.0/4.11,Compaq Tru64,DG-UX 5.6,AIX 4.3/4.2.1,ULTRIX 和 OpenVMS 等系统会将差错报文中的 UDP 头部的校验和字段置为 0。另外的一些系统则会保持 UDP 校验和不变。

③ ICMP 差错报文的“优先权”字段。IP 头部中有一个 8 位的 TOS 字段,TOS 字段包括一个 3 位的优先权字段、4 位的 TOS 子字段和一位必须置 0 的未用位,如图 12-7 所示。表 12-2 列出了优先权字段的定义。

01234567
优先权 TOSMBZ

0　1　2	3　4　5　6	
优先权	TOS	MBZ

图 12-7　IP 头部的 TOS 字段

表 12-2　优先权字段值

优 先 权	定　　义	优 先 权	定　　义
0	Routine (Normal)	4	Flash Override
1	Priority	5	Critical
2	Immediate	6	Internetwork Control
3	Flash	7	Network Control

RFC1812 对 IPv4 的路由设备做了规定,其中涉及对优先权字段的规定:ICMP“源端被关闭”(类型 4)差错报文必须将自己的优先权设置成和造成这一差错的报文的优先权一致。所有其他 ICMP 差错报文(目的不可到达、重定向、超时、参数问题)应该将它们的优先权设置为 6 或者 7。这些差错报文的 IP 优先权值是可设置的。

Arkin 的研究发现,除了 Linux,其他所有操作系统都将 0 作为 ICMP 差错报文的优先权值,而 Linux 使用 6 作为 ICMP 差错报文的优先权值(即使用 0xC0 作为 IP 头部 TOS 字节的值)。

④ ICMP 差错报文 IP 头部的不分片(DF)位。

有一些操作系统在发送 ICMP 差错报文时,会根据引起差错的数据报的 IP 头部的 DF 位来设置差错报文本身 IP 头部的 DF 位。Linux,ULTRIX,Novell Netware,HPUX,Windows 98/98SE/ME,Windows NT4 Server SP6 和 Windows 2000 Family 等系统则不会这么做。

⑤ ICMP 报文 IP 头部的 TTL 字段。

不同的操作系统在设置 ICMP 报文 IP 头部的 TTL 字段时有不同的默认值。而且一般来讲，ICMP 应答报文和 ICMP 查询报文的 TTL 还不一样。例如，Windows 95 应答报文和查询报文的 TTL 都是 32；Windows 98/98SE/ME/NT4 应答报文的 TTL 是 128、查询报文的 TTL 是 32；Windows 2000 应答报文和查询报文的 TTL 都是 128。

⑥ 使用代码字段不为 0 的 ICMP 回显请求。

ICMP 报文的种类由第一个字节（类型字段）和第二个字节（代码字段）决定。回显请求的类型字段为 8，默认的代码字段为 0。如果把回显请求的代码字段设置为非 0 值，这样的回显请求就不是标准的 ICMP 报文了。对于这样的回显请求报文，Windows 操作系统做出的回显应答（类型为 0）的代码字段值为 0，而其他系统和网络设备做出的回显应答的代码字段值和它收到的回显请求中的代码字段值相同。

⑦ TOS 子字段回显。

RFC1349 定义了 ICMP 报文使用 TOS 子字段的方法。其中区分了差错报文、查询报文和应答报文的不同使用方法，规则是：差错报文总是使用默认值 0；查询报文可以在 TOS 子字段中使用任何值；应答报文应该在 TOS 子字段中使用造成应答的查询报文中使用的 TOS 值。然而有些操作系统（如 Linux）在发送回显应答报文时忽视了这项规定，无论查询报文使用何种 TOS 值，它的应答报文的 TOS 值都是一样的。

（2）TCP 报文响应分析

这种技术通过区分不同操作系统对特定 TCP 报文（标准或非标准）的不同反应，实现对操作系统的区分。使用这种技术的代表有 Queso 和 Nmap（Nmap 其实也使用了一些 ICMP 响应分析的技巧）。下面将分别说明 Nmap 使用的操作系统探测技巧。

① FIN 探测。前面讲端口扫描的技巧时曾提到，“FIN 扫描通常只工作在基于 UNIX 的 TCP/IP 协议栈上”，这就可以用来作为一个探测操作系统的判断依据。

② 伪标记位探测。TCP 报文的头部有 8 个标记位。使用“伪标记位”（BOGUS Flag），即把 SYN 报文的 CWR 标记位的左边一位置 1，然后将这样的非标准 SYN 报文发给目标 TCP 端口。低于 2.0.35 版本的 Linux 内核会在回应包中保持这个标记，而其他操作系统似乎都没有这个问题。不过有的操作系统在收到这样的 SYN/BOGUS 报文时会发送一个 RST 复位连接。

③ TCP ISN 取样。

其原理是在操作系统对连接请求的回应中寻找 TCP 连接初始化序列号（ISN）的特征。目前可以区分的类别有传统的 64000 方式（旧 UNIX 系统使用）、随机增加方式（新版本的 Solaris、IRIX、FreeBSD、Digital UNIX、Cray 和其他许多系统使用）、真“随机”方式（Linux 2.0.* 及更高版本、OpenVMS 和新版本的 AIX 等操作系统使用）等。Windows 平台（还有其他一些平台）使用“基于时间”方式产生的 ISN 会随着时间的变化而呈相对固定的增长。另外还有一些系统总是使用固定的 ISN，如某些 3Com 集线器（使用 0x83）和 Apple LaserWriter 打印机（使用 0xC7001）。根据计算 ISN 的变化、最大公约数和其他一些有迹可循的规律，还可以将这些类别分得更细、更准确。

④ DF 位监视。

许多操作系统逐渐开始在它们发送的 IP 数据报中设置 DF 位，从而有益于提高传输性

能。但并不是所有操作系统都进行这种设置,或者有的系统只是在某些情况下使用这种设置。因此通过留意这个标记位的设置可以搜集到关于目标主机操作系统的更多有用信息。

⑤ TCP 初始化窗口大小。

这种技巧就是得到目标的初始化 TCP 窗口大小。有的操作系统总是使用比较特殊的值。例如 AIX 是唯一使用 0x3F25 窗口值的操作系统。而在 OpenBSD、FreeBSD 和 Windows 2000/XP 的 TCP 堆栈中,使用的窗口值总是 0x402E。

⑥ ACK 值。

不同协议栈实现在 TCP 报文的 ACK 值的选择上也存在差异。例如,假设向一个关闭的 TCP 端口发送一个 FIN/PSH/URG 报文,许多操作系统会将 ACK 值设置为 ISN 值,但 Windows 和某些打印机会设置为接收到的报文的 SEQ+1。如果向打开的端口发送 SYN/FIN/URG/PSH 报文,Windows 的返回值就会非常不确定,有时是接收到的报文的 SEQ 值,有时是 SEQ++,而有时回送的是一个似乎很随机的数值。

⑦ 片段处理。

不同操作系统在处理 IP 片段重叠时采用了不同的方式。有些用新的内容覆盖旧的内容,有些是以旧的内容为优先。有很多探测方法能确定这些包是如何重组的,从而能帮助确定操作系统类型。

⑧ TCP 选项。这是搜集信息的最有效方法之一。其基于以下原因:

- 它们通常是"可选的",因此并不是所有的操作系统都使用它们。
- 向目标主机发送带有可选项标记的数据包时,如果操作系统支持这些选项,会在返回包中也设置这些标记。
- 可以一次在数据包中设置多个可选项,从而增加了探测的准确度。

(3) TCP 报文延时分析

这是利用了 TCP 报文重传的特性。这种方法的具体实现是在"3 次握手"的过程中放弃对远程主机 SYN/ACK 报文的确认,迫使其重传,通过测量重传 TCP 报文之间的延时序列,获取远程操作系统指纹。图 12-8 说明了延时序列的意义。采用这种方法的代表是 RING。这种技术的最大优势就是它只需要一个打开的端口。如果目标主机是被防火墙所保护的,那么很可能只开了一个端口,其他端口则是被过滤了的。而且这种技术是使用了一个标准的 TCP 数据报,它将不会对目标主机造成任何的不利影响。但是这种探测方式需要花比 nmap 或 Xprobe 更多的时间,这是测量连续数据报时间延迟的一个固有缺点。

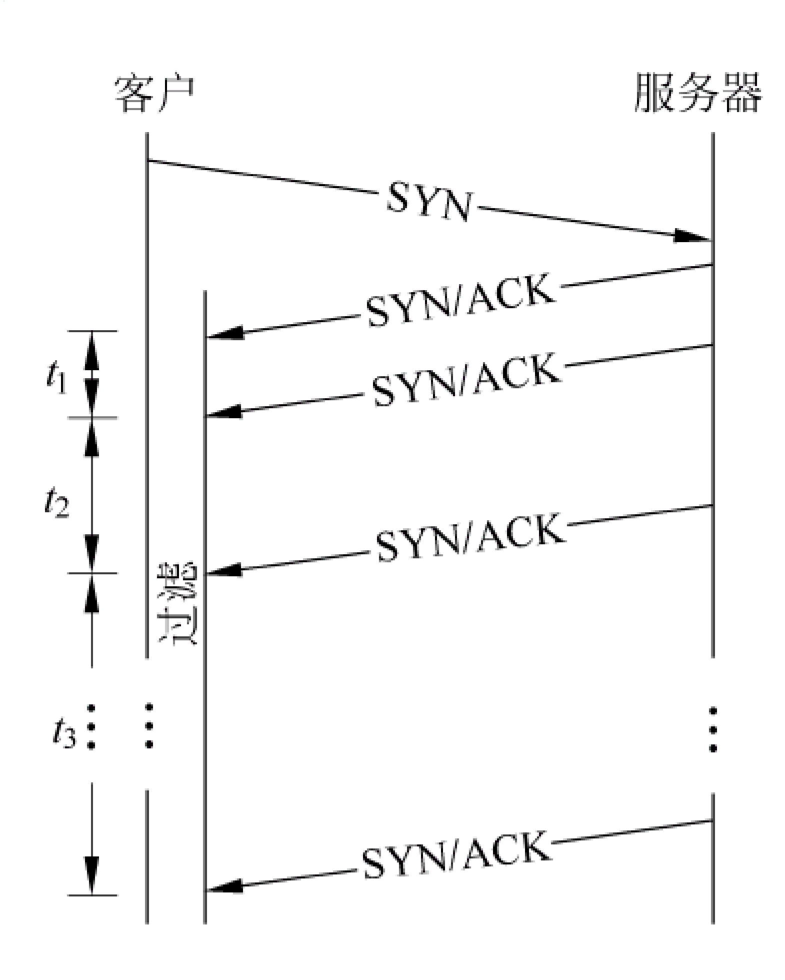


图 12-8　忽略 SYN/ACK 报文迫使服务器重传

下面的例子是使用 RING 探测操作系统类型。

```
\[root@ localhost ring\]# ./ring-d 192.168.1.128-s 192.168.1.12-p 111-i eth0
```

```
3558202 6000667 11999952 24200335
OS:Linux2.4
distance:1036218
```

(4) 被动协议栈指纹探测

被动的协议栈指纹探测和主动的协议栈指纹探测很相似,不同之处在于这种方法不主动向目标系统发送分组,而是通过嗅探目标网络的通信,抓取从远程主机上发送的数据报,获取包括 TTL、窗口大小、DF 位和服务类型等在内的数据报属性,构成目标系统的指纹。这种方法主要被入侵者使用,因为它不容易被发现。

表 12-3 比较了上述 5 种操作系统探测方法的优缺点。

表 12-3　操作系统探测方法比较

方　法		优　点	缺　点
利用系统和服务的 Banner		简单、快速、有效	不太可靠,有的情况下无法获得 Banner 信息,有时可能被 Banner 信息欺骗
主动特征探测	ICMP 响应分析	准确性较高	防火墙阻塞 UDP 或 ICMP 等协议时不太可靠
	TCP 报文响应分析	需要一个打开的 TCP 端口、一个关闭的 TCP 端口和一个关闭的 UDP 端口,准确性高	在有防火墙阻挡的情况下,可能只有一个开放的 TCP 端口,这时准确性大大降低
	TCP 报文延时分析	只需要一个打开的 TCP 端口	速度慢
被动特征探测		不易被发现,主要被入侵者使用	分析数据更加复杂

1223　漏洞检测

经过发现目标和攫取信息两个步骤以后,已经能够得到下面一些信息:目标网络上有哪些主机处于存活状态?这些主机上都运行什么系统?这些主机运行了哪些网络服务?而漏洞检测就是要回答最关键的一个问题——这些主机存在哪些漏洞?

根据漏洞的属性和利用方法,漏洞检测所要寻找的漏洞主要包括以下几个类别:

- 操作系统漏洞。
- 应用服务漏洞。
- 配置漏洞。

操作系统漏洞主要指操作系统本身由于实现中的问题而造成的漏洞。该类漏洞主要集中在系统网络协议栈的实现部分。由于涉及系统底层,往往很难弥补并容易造成重大影响。如著名的 teardrop 攻击利用的漏洞就是系统网络协议栈在处理 IP 包分片时候的错误。冲击波病毒也是利用的 Windows 系统 rpc 处理的漏洞。这种攻击往往可以造成整个操作系统的崩溃,不过由于操作系统往往比较成熟并经历了大量的测试,因此这种类型的漏洞相对较少,且使用这些漏洞所需的技术含量较高。

应用服务漏洞指各种应用服务在处理服务请求时存在的安全漏洞。相对于操作系统来说,应用服务由于种类繁多且具体的实现没有如操作系统那样经过广泛测试,往往存在

很多的问题。如对输入判断不够完全、开发中没有考虑安全防护、安全旁路等。目前的大部分漏洞检测行为主要针对这类应用服务漏洞。

配置漏洞指在对应用服务配置的过程中，由于忽略了安全要求而带来的安全漏洞。这些漏洞包括开放了不应公开的信息、安全保护薄弱化、安全旁路化等。其中比较典型的漏洞就是安全认证漏洞。漏洞检测一个很重要的部分就是扫描应用服务，通过字典猜测等方式，获取正确的用户登录密码，从而入侵系统。

漏洞检测的方法主要分为 3 种：直接测试(test)、推断(inference)和带凭证的测试(test with credentials)。

1. 直接测试

直接测试是指利用漏洞特点发现系统漏洞的方法。要找出系统中的常见漏洞，最显而易见的方法就是试图渗透漏洞。渗透测试是指使用针对漏洞特点设计的脚本或者程序检测漏洞。测试代码通常和渗透攻击代码类似，不同的是测试代码返回与“风险等级”对应的提示，而渗透攻击代码则直接向入侵者返回具有超级权限的执行环境。另外也有一些渗透攻击不返回任何东西，只是让系统处于易被攻击的状态，用户必须另外采取动作来判断是否有漏洞被渗透了。根据这一点，测试方法可以分为两种不同的类型：可以直接观察到的测试和只能间接观察到的测试。下面通过一个例子具体说明直接测试漏洞的方法。

IIS 5.0 具有一个 Unicode 解码漏洞，该漏洞的 CVE 名字为 CVE-2000-0884。该漏洞允许使用扩展 Unicode 代码取代“\\”和“/”字符，从而利用“../”遍历目录，这样用户可以通过构造特殊的 URL 远程执行系统上的任意命令。对于 IIS 而言，未经授权的用户可能利用 IUSR_machinename 账号的上下文空间访问任何已知的文件。该账号在默认情况下属于 Everyone 和 Users 组的成员，因此任何与 Web 根目录在同一逻辑驱动器上的、能被这些用户组访问的文件都能被删除、修改或执行，就如同一个用户成功登录所能完成的一样。没有安装 SP3 的 Windows 2000 系统都存在这个漏洞，当然，前提是它同时也正在提供 IIS 的 WWW 服务。

如果已知某主机正在提供 WWW 服务，为了检测该主机是否存在上述漏洞，可以直接利用渗透代码进行测试。这个漏洞的渗透代码也很简单：

```
http://target/scripts/..%c1%1c../path/file.ext
```

于是可以使用 Web 浏览器直接向目标主机发送一个请求：

```
http://target/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\\
```

如果 IIS 返回了 C:\\下的文件列表，则说明目标存在这个漏洞；如果返回的是 404 Object Not Found，则说明没有问题。这里使用了 dir 命令，这对目标系统是无害的，但是入侵者可以使用任何命令，包括 format，net 等命令，可以破坏硬盘数据或者添加用户等。

和上面的例子使用的方法类似，对于拒绝服务漏洞也可以直接使用渗透代码进行测试，所不同的只是测试 DoS 漏洞的渗透代码通常是经过编译的二进制代码。

直接测试的方法具有下面一些特点：

- 通常用于对 Web 服务器漏洞、拒绝服务漏洞进行检测；
- 能够准确地判断系统是否存在特定漏洞；
- 对于渗透所需步骤较多的漏洞速度较慢；
- 攻击性较强，可能对存在漏洞的系统造成破坏；
- 对于 DoS 漏洞，测试方法会造成系统崩溃；
- 不是所有漏洞的信息都能通过测试方法获得。

2 推断

推断是指不利用系统漏洞而判断漏洞是否存在的方法。它并不直接渗透漏洞，只是间接寻找漏洞存在的证据。采用推断方法的检测手段主要有版本检查（version check）、程序行为分析、操作系统堆栈指纹分析和时序分析等。

其中，版本检查是推断方法中最简单的一个应用。它依赖于服务器对请求响应的旗标获取系统的有关信息，然后将获得的版本号与已知信息比较，以判断目标系统是否是受漏洞影响的系统。如要检测 IIS 的 Unicode 解码漏洞，除了使用上面的直接测试方法，也可以使用版本检查的方法，如果检查到目标用的 IIS 版本是 5.1 或者更高，就可以推断目标不具有 Unicode 解码漏洞。

行为分析在需要推翻某个“风险假设”的时候非常有用。在这种情况下，它分析目标程序的行为，如果发现该程序的行为和具有漏洞的版本的程序行为不一致，就认为目标程序不存在漏洞。这种方法不如渗透测试方法可靠，但是攻击性更小。这种方法在推断没有公开细节的新漏洞时也很有用。另外，它也可以用于检查 DoS 漏洞，因为它基本没有攻击性，所以可以在检查很多 DoS 漏洞以后再重新启动系统。

推断方法有时也和测试方法结合使用，如首先推断出目标采用的系统类型，然后进行针对该系统的测试。

推断的方法在快速检查大量目标时很有用，因为这种方法对计算机和网络的要求都很低。而它最主要的缺点就是可靠性较低。

3. 带凭证的测试

凭证是指访问服务所需要的用户名或者密码，包括 UNIX 的登录权限和从网络调用 Windows NT 的 API 的能力。

除了目标主机 IP 地址以外，直接测试和推断两种方法都不需要其他任何信息。然而，很多攻击都是由拥有 UNIX shell 访问权限或者 NT 资源访问权限的用户发起的，他们的目标在于将自己的权限提升成为超级用户，从而可以执行某个命令。对于这样的漏洞，前面两种方法很难检查出来。因此，如果赋予测试进程目标系统的角色，将能够检查出更多的漏洞。这种方法就是带凭证的测试。

由于拥有了目标主机的证书，一些原来只能由本地扫描发现的漏洞就能够通过网络安全扫描发现了。然而需要注意的是，由于拥有了目标主机的证书，检测系统本身的安全就更加值得注意，因为入侵者可能从检测系统上得到目标系统的访问权限。所以一个好的检测系统应该集成对自己进行扫描的功能；否则，漏洞扫描有可能变得很危险。

12.3 常用的网络扫描工具

网络扫描的一些常用工具都是可以从 Internet 上免费获得的。在使用这些工具之前请一定确认目标网络已经授权你对其进行扫描。因为这些工具有可能对扫描的目标造成危害。

1. Netcat

由 Hobbit(hobbit@avian.org)编写的 Netcat(或称 nc)是一个优秀的实用工具，Weld Pond(weld@10pht.com)将其移植到了 NT 平台上。它能执行的任务是如此之多，以至于被称为网络工具箱中的“瑞士军刀”。

2. 网络主机扫描程序 Nmap

由 Fyodor(fyodor@insecure.org)编写的 Nmap(www.nmap.org)是一个开放源码的网络扫描工具。Nmap 实现了前面提到的绝大部分的扫描技巧和操作系统探测技巧，可以用来发现网络上存活的主机、这些主机开放了哪些 TCP 和 UDP 端口、这些主机运行什么样的操作系统，以及操作系统的版本、正在使用什么样的防火墙和过滤设备等信息。

3. SATAN

前面的两个工具主要是用于发现目标和攫取信息两个阶段，而一次完整的漏洞扫描还应该包括“漏洞检测”这个阶段。SATAN 即“网络分析的安全管理工具”。它提供一整套安全管理、测试和报告的功能，可以用来搜集网络上主机的许多信息，可以识别并且自动报告与网络相关的安全问题。

4. nessus

nessus 是一个功能强大而又易于使用的网络漏洞扫描工具，运行于 POSIX 系统(Solaris，FreeBSD 和 GNU/Linux 等)。它不仅免费而且更新很快。该系统被设计为客户/服务器模式，服务器端负责进行安全扫描，客户端用来配置、管理服务器端、客户端和服务器端之间的通信使用 SSL 加密。

5. X-scan

X-scan 是由“安全焦点”开发的一个免费的漏洞扫描工具，运行于 Windows 操作系统。采用多线程方式对指定 IP 地址段(或单机)进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式。

12.4 不同的扫描策略

前面介绍了网络扫描的原理、技术和工具。然而对计算机进行安全扫描不仅可以从网络进行，也可以从主机进行。也就是说安全扫描有基于网络和基于主机两种策略。

(1) 基于网络的安全评估工具从入侵者的角度评估系统，这类工具叫作远程扫描器或者网络扫描器。基于主机的安全评估工具从本地系统管理员的角度评估系统，这类工具叫作本地扫描器或者系统扫描器。这两类扫描器的主要目的都是发现系统或网络潜在的安全漏洞。然而由于其着眼点和实现方式不同，两者的特点也各有千秋。

(2) 基于主机的脆弱性评估分析文件内容，对系统中不合适的设置、脆弱的口令及其他同安全规则抵触的对象进行检查。它具有以下特点：

- 运行于单个主机，扫描目标为本地主机；
- 扫描器的设计和实现与目标主机的操作系统相关；
- 可以在系统上任意创建进程；
- 扫描项目主要包括用户账号文件、组文件、系统权限、系统配置文件、关键文件、日志文件、用户口令、网络接口状态、系统服务和软件脆弱性等。

基于网络的脆弱性评估通过执行一些插件或者脚本模拟对系统进行攻击的行为并记录系统的反应，从而发现其中的漏洞。它具有以下特点：

- 运行于单个或多个主机，扫描目标为本地主机或者单/多个远程主机；
- 扫描器的设计和实现与目标主机的操作系统无关；
- 通常的网络安全扫描不能访问目标主机的本地文件(具有目标主机访问权限的扫描除外)；
- 扫描项目主要包括目标的开放端口、系统网络服务、系统信息、系统漏洞、远程服务漏洞、特洛伊木马检测和拒绝服务攻击等。

基于主机的脆弱性评估可以更准确地定位系统的问题，发现系统的漏洞；然而缺点是平台相关、升级复杂，而且扫描效率较低(一次只能扫描一台主机)。基于网络的脆弱性评估从入侵者的角度进行检测，能够发现系统中最危险、最可能被入侵者渗透的漏洞，扫描效率更高，而且由于与目标平台无关，通用性强，安装简单；缺点是不能检查不恰当的本地安全策略，另外也可能影响网络性能。

12.5　本章小结

计算机漏洞是系统的一组特性，恶意的主体(攻击者或者攻击程序)能够利用这组特性，通过已授权的手段和方式获取对资源的未授权访问，或者对系统造成损害。

从技术角度而言，漏洞的来源主要有软件或协议设计时的瑕疵、软件或协议实现中的弱点、软件本身的瑕疵、系统和网络的错误配置。

一次完整的网络扫描主要分为 3 个阶段：目标发现、信息攫取和漏洞检测。

目标发现阶段的技术主要有 ICMP 扫射、广播 ICMP、非回显 ICMP、TCP 扫射和 UDP 扫射。

端口扫描的主要技术有 TCP connect( ) 扫描、TCP SYN 扫描、TCP ACK 扫描、TCP FIN 扫描、TCP XMAS 扫描、TCP 空扫描、FTP 反弹扫描(FTP Bounce Scan)和 UDP 扫描。

远程操作系统识别的主要方法有系统服务旗标识别、主动协议栈指纹探测(ICMP 响应分析、TCP 报文响应分析和 TCP 报文延时分析)和被动协议栈指纹探测。

漏洞检测的主要方法有直接测试(test)、推断(inference)和带凭证的测试(test with credential)。

基于网络的安全评估工具从入侵者的角度评估系统,这类工具叫作远程扫描器或者网络扫描器。基于主机的安全评估工具从本地系统管理员的角度评估系统,这类工具叫作本地扫描器或者系统扫描器。这两类扫描器的主要目的都是发现系统或网络潜在的安全漏洞。然而由于其着眼点和实现方式不同,两者的特点也各有千秋。

习　题

1. 计算机系统会被黑客攻击的最根本原因是什么?网络攻击的本质是什么?
2. 在 CERT/CC 的网站上查找 2002 年报告的漏洞数量。
3. 在 Internet 上查找现在最新的 SANS/FBI 最危险的 20 个漏洞列表。
4. 简述计算机脆弱性的概念和产生原因。
5. 什么是 CVE 和 Bugtraq?
6. 在 CVE 的网站上查找名字为 CVE-2000-0884 的漏洞描述。
7. 查找上述漏洞的 Bugtraq ID 及 Bugtraq 数据库中列出的受影响系统。
8. 简述网络安全扫描的内容和大致步骤。
9. 有哪些方法可以用来发现目标?各自的优缺点是什么?
10. 端口扫描的目的是什么?简述 TCP SYN 扫描的原理。
11. 什么是操作系统的 TCP/IP 协议栈指纹?探测远程操作系统类型有哪些方法?
12. 漏洞检测的方法主要有哪 3 种?
13. 检测拒绝服务漏洞可以使用哪些方法?比较这些方法的优缺点。
14. Nmap 通过什么判断远程操作系统类型?
15. nessus 的插件有什么用?
16. 基于主机的扫描和基于网络的扫描有什么不同?

第13章 入侵检测

本章要点：

- 入侵检测的概念；
- 入侵检测系统分类；
- 入侵检测系统分析方式；
- 入侵检测系统的设置与部署；
- 入侵检测系统的优缺点。

13.1 入侵检测概述

13.1.1 入侵检测的概念

入侵检测是从计算机网络或计算机系统中的若干关键点搜集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象的一种机制。入侵检测系统的英文缩写是IDS(intrusion detection system)，它使用入侵检测技术对网络与其上的系统进行监视，并根据监视结果进行不同的安全动作，最大限度地降低可能的入侵危害。简单地说，入侵检测系统是这样工作的：若有一个计算机系统，它与网络连接着，或许也同Internet连接，由于一些原因，允许网络上的授权用户访问该计算机。例如，有一个连接着Internet的Web服务器，允许一定的客户、员工和一些潜在的客户访问存放在该Web服务器上的Web页面。然而，不希望其他员工、顾客或未知的第三方的未授权访问。一般情况下，可以采用一个防火墙或者一些类型的认证系统阻止未授权访问。然而，有时简单的防火墙措施或者认证系统可能被攻破。入侵检测是一系列在适当的位置上对计算机未授权访问进行警告的机制。对于假冒身份的入侵者，入侵检测系统也能通过与其他安全设备的联动，采取一些措施来拒绝其访问。

入侵检测系统基本上不具有访问控制的能力，它就像是一个有着多年经验、熟悉各种入侵方式的网络侦察员，通过对数据包流的分析，可以从数据流中过滤出可疑数据包，通过与已知的入侵方式进行比较，确定入侵是否发生以及入侵的类型并进行报警。网络管理员可以根据这些报警确切地知道所受到的攻击并采取相应的措施。可以说，入侵检测系统是网络管理员经验积累的一种体现，它极大地减轻了网络管理员的负担，降低了对网络管理员的技术要求，提高了网络安全管理的效率和准确性。

目前，大部分网络攻击在攻击前有资料搜集的过程，例如，基于特定系统的漏洞攻击，在攻击之前需要进行端口扫描，以确认系统的类型以及漏洞相关的端口是否开启。某些

攻击在初期就可以表现出较为明显的特征，例如，假冒有效用户登录，在攻击初期的登录尝试具有明显的特征。对于这两类攻击，入侵检测系统可以在攻击的前期准备时期或是在攻击刚刚开始的时候进行确认并发出警报。入侵检测系统还可以对报警的信息进行记录，为以后的一系列实际行动提供证据支持，形成入侵行为的完整证据链。这就是入侵检测系统的预警功能。

入侵检测一般采用旁路侦听的机制，因此不会产生对网络带宽的大量占用，系统的使用对网内外的用户来说是透明的，不会有任何的影响。入侵检测系统的单独使用不能起到保护网络的作用，也不能独立地防止任何一种攻击。但它是整个网络安全系统的一个重要的组成部分，它所扮演的是网络安全系统中侦察与预警的角色，协助网络管理员发现并处理任何已知的入侵。可以说，它是对其他安全系统有力的补充，弥补了防火墙在高层上的不足。通过对入侵检测系统所发出警报的处理，网络管理员可以有效地配置其他安全产品，以使整个网络安全系统达到最佳的工作状态，尽可能降低因攻击而带来的损失。

随着技术的不断进步，成熟的入侵检测技术也应用到了实时网络防护领域。入侵防护以入侵检测技术为基础，依托高性能硬件，实现对数据包的高层应用分析，针对可能存在的应用攻击行为，实时进行阻断与数据丢弃，提高了网络对安全事件响应的实时性，更好地保护主机的安全。

13.1.2　入侵检测系统的基本结构

CIDF(common intrusion detection framework，网址 http：//www.gidos.org/)阐述了一个入侵检测系统的通用模型，如图 13-1 所示。CIDF 将入侵检测系统需要分析的数据统称为事件(event)，事件可以是网络中的数据包，也可以是从系统日志等其他途径得到的信息。它将入侵检测系统分为以下组件。

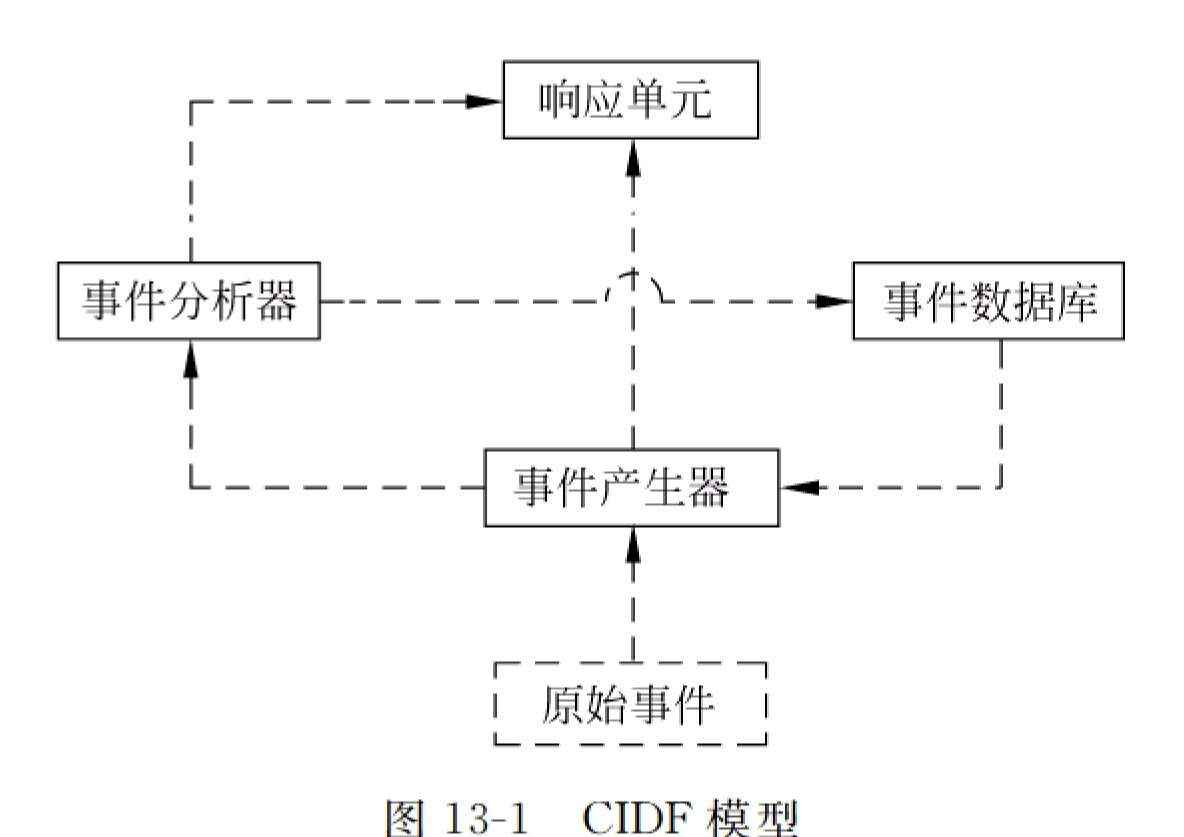


图 13-1　CIDF 模型

(1) 事件产生器

事件产生器采集和监视被保护系统的数据，这些数据可以是网络的数据包，也可以是从系统日志等其他途径搜集到的信息。并且将这个数据进行保存，一般是保存到数据库中。

(2) 事件分析器

事件分析器的功能主要分为两个方面：一是用于分析事件产生器搜集到的数据，区

分数据的正确性,发现非法的或者具有潜在危险的、异常的数据现象,通知响应单元做出入侵防范;二是对数据库保存的数据做定期的统计分析,发现某段时期内的异常表现,进而对该时期内的异常数据进行详细分析。

(3) 响应单元

响应单元是协同事件分析器工作的重要组成部分,一旦事件分析器发现具有入侵企图的异常数据,响应单元就要发挥作用,对具有入侵企图的攻击施以拦截、阻断、反追踪等手段,保护被保护系统免受攻击和破坏。

(4) 事件数据库

事件数据库记录事件分析单元提供的分析结果,同时记录所有来自于事件产生器的事件,用来进行以后的分析与检查。

13.2 入侵检测系统分类

根据入侵检测系统的检测对象,入侵检测系统主要分为两大类:基于主机的入侵检测系统和基于网络的入侵检测系统。而根据工作方式的不同,基于网络的入侵检测系统还分为旁路入侵检测系统和主干入侵防护系统。除此之外,还有基于内核的高性能入侵检测系统和两大类相结合的入侵检测系统,这些类别是两个主要类别的引申和综合。

13.2.1 基于主机的入侵检测系统

基于主机的入侵检测系统用于保护单台主机不受网络攻击行为的侵害,需要安装在被保护的主机上。这一类入侵检测系统直接与操作系统相关,它控制文件系统以及重要的系统文件,确保操作系统不会被随意地删改。该类入侵检测系统能够及时发现操作系统所受到的侵害,并且由于它保存一定的校验信息和所有系统文件的变更记录,所以在一定程度上还可以实现安全恢复机制。

按照检测对象的不同,基于主机的入侵检测系统可以分为两类:网络连接检测和主机文件检测。

1. 网络连接检测

网络连接检测是对试图进入该主机的数据流进行检测,分析确定是否有入侵行为,避免或减少这些数据流进入主机系统后造成损害。

网络连接检测可以有效地检测出是否存在攻击探测行为,攻击探测几乎是所有攻击行为的前奏。系统管理员可以设置好访问控制表,其中包括容易受到攻击探测的网络服务,并且为它们设置好访问权限。如果入侵检测系统发现有对未开放的服务端口进行网络连接,说明有人在寻找系统漏洞,这些探测行为就会被入侵检测系统记录下来,同时这种未经授权的连接也被拒绝。

2 主机文件检测

通常入侵行为会在主机的各种相关文件中留下痕迹，主机文件检测能够帮助系统管理员发现入侵行为或入侵企图，及时采取补救措施。

主机文件检测的检测对象主要包括以下几种：

（1）系统日志

系统日志文件中记录了各种类型的信息，包括各用户的行为记录。如果日志文件中存在着异常的记录，就可以认为已经或正在发生网络入侵行为。这些异常包括不正常的反复登录失败记录、未授权用户越权访问重要文件、非正常登录行为等。

（2）文件系统

恶意的网络攻击者会修改网络主机上包含重要信息的各种数据文件，他们可能会删除或者替换某些文件，或者尽量修改各种日志记录来销毁他们的攻击行为可能留下的痕迹。如果入侵检测系统发现文件系统发生了异常的改变，例如一些受限访问的目录或文件被非正常地创建、修改或删除，就可以怀疑发生了网络入侵行为。

（3）进程记录

主机系统中运行着各种不同的应用程序，包括各种服务程序。每个执行中的程序都包含了一个或多个进程。每个进程都存在于特定的系统环境中，能够访问有限的系统资源、数据文件等，或者与特定的进程进行通信。黑客可能将程序的进程分解，致使程序中止，或者令程序执行违背系统用户意图的操作。如果入侵检测系统发现某个进程存在着异常的行为，就可以怀疑有网络入侵。

（4）系统运行控制

目前的操作系统，尤其是主流操作系统，在安全防护上都存在一定程度的不足。针对系统的运行特性，主机入侵检测系统参与系统的运行过程，采取措施防止缓冲区溢出，增加文件系统的保护，封闭信号，从而使得入侵者破坏系统越来越困难。同时采取一些步骤阻止根用户的一些活动，例如安装一个包嗅探器或改变防火墙策略。

Tripwire 就是一种基于主机文件的入侵检测系统，它为主机系统的一些关键文件建立一个高效的校验和，并且根据文件的正常变化进行维护。通过将这些校验和与实际文件进行比较，来检测是否存在对文件及其属性的异常修改，从而发现网络入侵行为，并且能够在一定程度上恢复修改前的系统文件。

在 Linux 上主要有两种主机入侵检测系统：OpenWall 和 LIDS。它们与 Linux 系统很好地结合，防止系统被非法使用与破坏。

可能有些人觉得像 Tripwire 这样的系统并不是很有用。但是，一旦系统被外界的入侵者破坏并需要关闭和重新建设该系统，就会发觉监视文件系统以发现滥用的征兆是令人非常乐意接受的。破坏已经产生了，系统的完整性没有办法得到保证，所以最好的办法是用提供商提供的原来版本的光盘重新构建操作系统。而 LIDS 提供的方法能保护系统不被破坏，因此更具有吸引力。

基于主机的入侵检测系统具有以下优点：

- 检测准确度较高；

- 可以检测到没有明显行为特征的入侵；
- 能够对不同的操作系统进行有针对性的检测；
- 成本较低；
- 不会因网络流量影响性能；
- 适于加密和交换环境。

基于主机的入侵检测系统具有以下不足：

- 实时性较差；
- 无法检测数据包的全部；
- 检测效果取决于日志系统；
- 占用主机资源；
- 隐蔽性较差；
- 入侵检测系统本身的文件也是系统安全的薄弱点，如果操作系统权限管理较差，入侵者能够修改重要的信息文件，这种入侵检测系统将无法起到预期的作用。

13.2.2　基于网络的入侵检测系统

基于网络的入侵检测系统通常是作为一个独立的个体放置于被保护的网络上，它使用原始的网络分组数据包作为进行攻击分析的数据源，一般利用一个网络适配器来实时监视和分析所有通过网络进行传输的通信。一旦检测到攻击，入侵检测系统应答模块通过通知、报警以及中断连接等方式来对攻击做出反应。

基于网络的入侵检测可以侦听某一个 IP，保护特定服务器的安全，也可以侦听整个网段。为了能够对整个网段进行侦听，系统会将本身的网卡设置为混杂模式以接收网段内的所有数据包。通常系统会使用位于网络层和传输层的网络侦听底层实现对网络的侦听。它们的主要任务就是获取其所见到的所有包并传给上一层。

获取包的主要目的是要对它进行处理以获得需要的信息。最常用的处理是数据包的流量统计以及数据包的归类分析。以前，系统管理员可以通过对数据包的分析，了解到系统是否存在被攻击的情况或是否存在非法的访问。这项工作如果单纯由网络管理员来做，就会耗费大量的时间，同时也对网络管理员提出了更高的要求。使用入侵检测系统可以较好地解决这个问题。通过多年的总结，人们发现大多数的入侵都有一定的特征。只要在数据包记录中发现这种有特征的行为，就可以在一定程度上断定发生了或即将发生入侵。入侵检测系统就是通过将实际的数据流量记录与入侵模式库中的入侵模式进行匹配，寻找可能的攻击特征。如果是正常数据包，则允许通过或留待进一步分析；如果是不安全的数据包，则可以进行阻断网络连接等操作，在这种情况下，还可以重新配置防火墙以阻断相应的网络连接，共同保护主机的安全。大体上，基于网络的入侵检测系统主要经过了以下几个发展阶段：

1. 包嗅探器和网络监视器

最初设计包嗅探器和网络监视器的目的是帮助监视以太网络的通信。最早有两种产

品：Novell LANalyser 和 Network Monitor。这些产品抓获所有网络上能够看到的包。一旦抓获了这些数据包，就可以进行以下工作：

(1) 对包进行统计。统计通过的数据包，并统计该时期内通过的数据包的总的大小(包括总的开销，如包的报头)，就可以很好地知道网络的负载状况。LANalyser 和 Network Monitor 都提供了网络相关负载的图形化或图表表现形式。

(2) 详细地检查包。例如，可以抓获一系列到达 Web 服务器的数据包来诊断服务器的问题。

近年来，包嗅探产品已经成了独立的产品。程序(例如 Ethereal 和 Network Monitor 的最新版本)可以对内部各种类型的包进行拆分，从而可以知道包内部发生了什么类型的通信。

这些工具同时也能用来进行破坏活动。例如，通过嗅探连接到一台机器的 Telnet 包，包嗅探器能够用来发现系统用户 UNIX 密码。一个攻击者一旦危害网络，他们要做的第一件事就是安装一些包嗅探器。

所有的包嗅探器都要求网络接口运行在混杂模式下。只有运行在混杂模式下，包嗅探器才能接收通过网络接口卡的每个包。在安装包嗅探器的机器上运行包嗅探器通常需要管理员的权限，这样，网卡的硬件才能被设置为混杂模式。

另外需要考虑的一点是包嗅探器在交换机上的使用，在一个网络中，它比集线器使用得更多。注意，在交换机的一个接口上收到的数据包不总是被送向交换机的其他接口。由于这种原因，包嗅探器在交换网络环境下通常不能正常工作，需要交换机配置镜像端口来专门提供包嗅探功能。

2 基于网络的入侵检测

从安全的观点来看，包嗅探器所带来的好处很少。抓获网络上的每个数据包，拆分该包，根据包的内容手工采取相应的反应，太浪费时间了，尤其是对于那些天天在外进行网络培训的人员而言，从大量积累数据中获取有价值的信息非常困难。

ISS RealSecure Engine 和 Network Flight Recorder 是基于网络入侵检测的两种类型软件包。RealSecure Engine 能够执行的入侵检测是检查通过网络的数据包。对于合法的数据包，允许它们通过(为了今后的分析，也可以对它们进行记录)。当一个数据包危及到目标系统的安全或完整性时，同时向目标系统和发送该数据包的系统发送 TCP “Connection Closed”或 ICMP“port unreachable”来阻止该包的传送。

此外，基于网络的入侵检测系统可以执行以下任务：

(1) 检测端口扫描。在攻击一个系统时，一个入侵者通常对该系统进行端口扫描，从而判断存在哪些脆弱性。企图对 Internet 上的一台主机进行端口扫描通常是一个人要试图破坏网络的一个信号。

(2) 检测常见的攻击行为。访问 Web 服务器的 80 端口通常被认为是无害的活动，但是，一些访问企图事实上是故意在进行攻击，或者试图攻击。例如，一个像“GET/../../..etc/passwd HTTP/1.0”这样的访问或许是一个不好的征兆，必须封锁。

(3) 识别各种各样可能的 IP 欺骗攻击。用来将 IP 地址转化为 MAC 地址的 ARP 协

议通常是一个攻击目标。通过在以太网上发送伪造的 ARP 数据包，已经获得系统访问权限的入侵者可以假装是一个不同的系统在进行操作。这将导致各种各样的拒绝服务攻击，也叫系统劫持。一个重要的服务器（如 DNS 服务器或者认证服务器）是如何被欺骗的呢？入侵者可以使用这种欺骗将数据包重定向到自己的系统，并在安全的网络上进行中间人类型的攻击。通过记录 ARP 数据包，基于网络的入侵检测系统就能识别出受害的源以太网地址，并判断是否是一个破坏者。

（4）当检测到一个不希望的活动时，基于网络的入侵检测系统将采取行动，包括干涉从入侵者处发来的通信，或重新配置附近的防火墙策略以封锁从入侵者的计算机或网络发来的所有通信。

基于网络的入侵检测系统有以下优点：

- 可以提供实时的网络行为检测；
- 可以同时保护多台网络主机；
- 具有良好的隐蔽性；
- 有效保护入侵证据；
- 不影响被保护主机的性能以及服务的正常提供。

基于网络的入侵检测系统有以下不足：

- 防入侵欺骗的能力通常较差；
- 在交换式网络环境中难以配置；
- 检测性能受硬件条件限制；
- 不能处理加密后的数据。

13.2.3　入侵防护系统

入侵防护系统（intrusion protection system，IPS）是网络入侵检测系统的一种特殊形式。从安全防护的地位上来看，入侵防护系统已经超出了入侵检测系统的范围。它是网络高层应用防护设备，是安全防护产品的进一步拓展。

入侵防护系统主要采用入侵检测技术实现网络防护功能，在网络位置上，入侵防护系统位于网络主干位置，一般以透明网关形式存在。所有的进出网络的数据包均需要通过入侵防护系统。因此入侵防护系统有时也被称为嵌入式 IDS 或网关 IDS。

入侵防护系统从链路层获取网络数据，使用入侵检测技术对数据包进行分析，对其中的高层应用协议数据进行重组与协议追踪。对存在问题的数据包，则处理该数据包并关闭相应连接，而正常的数据包则通过另一网卡通过。对于存在问题的数据包，入侵防护系统通常的做法是直接丢弃，也可以采用修改重建、报警等响应方式。通过对问题数据的实时阻断，入侵防护系统可以在第一时间阻断攻击行为，防止受保护服务器受到攻击。通过对攻击行为的过滤，保证了服务器的稳定运行，提高了整个网络系统的可靠性。

入侵防护系统核心采用了网络入侵检测技术，由于目前硬件和软件技术条件的限制，入侵防护系统通常是防火墙技术与入侵检测技术相结合的产物。通过防火墙技术过滤大部分数据，对于关键应用，如 Web 应用、邮件应用、文件共享应用等，根据应用端口选择性上传到入侵检测核心，根据分析结果，决定是否继续传送。

由于入侵检测技术对运算性能要求较高,目前成形的入侵防护产品以硬件形式的居多。通过将入侵检测的成熟技术——特征匹配技术固化在硬件中,提高对单包数据分析的能力,实现基于单包的网络入侵防护。这种硬件入侵防护系统可以适应高带宽的网络要求,对于自动型网络攻击行为具有较好的防护能力。而软件入侵防护产品虽然可以实现更复杂的协议跟踪检测,但由于受性能限制,很难在高带宽环境下有效工作。

网络入侵防护系统有以下优点:

- 实时阻断网络攻击;
- 隐蔽数据检测,对通信双方完全透明;
- 主干检测,保证数据百分之百的捕获,避免出现绕过攻击的情况;
- 透明模式,不会对网络拓扑造成影响。

网络入侵防护系统有以下不足:

- 分析效率较低,无法适应高速网络环境;
- 继承了入侵检测的误报缺陷,易造成对正常网络通信的影响;
- 为了尽可能地降低误报率,造成漏报情况较多,只能对能够准确确认的攻击进行处理;
- 无法检测加密环境数据。

13.2.4 两种入侵检测系统的结合运用

基于网络的入侵检测系统和基于主机的入侵检测系统都有各自的优势和不足,这两种方式各自都能发现对方无法检测到的一些网络入侵行为,如果同时使用互相弥补不足,会起到良好的检测效果。

例如,从某个重要服务器的键盘发出的攻击并不经过网络,因此就无法通过基于网络的入侵检测系统检测到,只能使用基于主机的入侵检测系统来检测。基于网络的入侵检测系统通过检查所有的数据包头来进行检测,而基于主机的入侵检测系统并不查看包头。基于网络的入侵检测系统可以研究负载的内容,查找特定攻击中使用的命令或语法,这类攻击可以被实时检查包序列的入侵检测系统迅速识别;而基于主机的入侵检测系统无法看到负载,因此也无法识别嵌入式的负载攻击。又如,基于主机的入侵检测系统使用系统日志作为检测依据,因此它们在确定攻击是否已经取得成功时,与基于网络的检测系统相比具有更大的准确性。在这方面,基于主机的入侵检测系统对基于网络的入侵检测系统是一个很好的补充,可以使用基于网络的入侵检测系统提供早期报警,使用基于主机的入侵检测系统来验证攻击是否取得成功。

13.2.5 分布式的入侵检测系统

目前的入侵检测系统一般采用集中式模式,在被保护网络的各个网段中分别放置检测器进行数据包搜集和分析,各个检测器将检测信息传送给中央控制台进行统一处理,中央控制台还会向各个检测器发送命令。这种模式的缺点是难以及时对在复杂网络上发起的分布式攻击进行数据分析以至于无法完成检测任务,入侵检测系统本身所在的主机还可能面临因为负荷过重而崩溃的危险。此外入侵检测系统一般采用单一的检测分析方

法，随着网络攻击方法的日趋复杂化，单一的基于异常检测或者误用检测的分析方法所获得的效果很难令人满意。此外，在大型网络中，网络的不同部分可能分别采用不同的入侵检测系统，各个入侵检测系统之间通常不能互相协作，不仅不利于检测工作，甚至还会产生新的安全漏洞。

对于上述问题，采用分布式结构的入侵检测模式是解决方案之一，也是目前入侵检测技术的一个研究方向。这种模式的系统采用分布式智能代理的结构，由一个或者多个中央智能代理和大量分布在网络各处的本地代理组成。其中本地代理负责处理本地事件，中央代理负责统一调控各个本地代理的工作以及从整体上完成对网络事件进行综合分析的工作。检测工作通过全部代理互相协作共同完成。

13.3　入侵检测系统的分析方式

入侵检测系统的检测分析技术主要分为两大类：异常检测和误用检测。下面将对它们的原理进行说明，同时列举相关的代表性技术并对技术的优缺点进行评价。

13.3.1　异常检测技术——基于行为的检测

1. 异常检测技术的基本原理

异常检测技术(anomaly detection)也称为基于行为的检测技术，是指根据用户的行为和系统资源的使用状况判断是否存在网络入侵。

异常检测技术首先假设网络攻击行为是不常见的或是异常的，区别于所有的正常行为。如果能够为用户和系统的所有正常行为总结活动规律并建立行为模型，那么入侵检测系统可以将当前捕获到的网络行为与行为模型相对比，若入侵行为偏离了正常的行为轨迹，就可以被检测出来。

异常检测技术先定义一组系统正常活动的阈值，如 CPU 利用率、内存利用率、文件校验和等，这类数据可以人为定义，也可以通过观察系统，用统计的办法得出，然后将系统运行时的数值与所定义的“正常”情况比较，得出是否有被攻击的迹象。这种检测方式的核心在于如何分析系统运行情况。

异常检测技术给系统对象(如用户、文件、目录和设备等)创建一个统计描述，统计正常使用时的一些测量属性(如访问次数、操作失败次数和延时等)。测量属性的平均值将用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生。例如，统计分析可能标识一个不正常行为，因为它发现一个在晚八点至次日早六点不登录的账户却在凌晨两点试图登录。

具体的统计分析方法，如基于专家系统的、基于模型推理的和基于神经网络的分析方法，目前正处于研究热点和迅速发展之中。

2 异常检测技术的评价

异常检测技术有以下优点：

- 能够检测出新的网络入侵方法的攻击；

- 较少依赖于特定的主机操作系统；
- 对于内部合法用户的越权违法行为的检测能力较强。

异常检测技术有以下不足：

- 误报率高；
- 行为模型建立困难；
- 难以对入侵行为进行分类和命名。

3. 异常检测技术分类

异常检测技术的核心问题是建立行为模型，目前主要有以下几种方法。

(1) 统计分析异常检测

统计分析异常检测方法在基于异常检测技术的入侵检测系统中使用最为广泛。首先要对系统或用户的行为按照一定的时间间隔进行采样，样本的内容包括每个会话的登录、退出情况，CPU 和内存的占用情况，硬盘等存储介质的使用情况等。对每次采集到的样本进行计算，得出一系列的参数变量来对这些行为进行描述，从而产生行为轮廓，将每次采样后得到的行为轮廓与已有轮廓进行合并，最终得到系统和用户的正常行为轮廓。入侵检测系统通过将当前采集到的行为轮廓与正常行为轮廓相比较，来检测是否存在网络入侵行为。在早期采用的算法中，系统计算出所有变量的平均值，然后根据平均偏差检测当前行为是否超过了某一阈值，这样的模型比较粗糙，检测精度较低。目前使用一种更加复杂的模型，检测系统同时计算并且比较每个用户长期和短期的活动状态，而状态信息随着用户行为的变化不断更新。

也可以采用下面的算法计算行为的异常程度。

$M_1, M_2, \cdots, M_n$ 表示行为轮廓中的特征变量，$S_1, S_2, \cdots, S_n$ 分别表示各个变量的异常性测量值，S_i 的值越大就表示异常性越大。a_i 表示变量 M_i 的权重值。将各个异常性测量值的平方加权求和得出特征值

$$M = a_1 S_1^2 + a_2 S_2^2 + \cdots + a_n S_n^2 \quad a_i > 0, \quad 1 \leqslant i \leqslant n$$

然后选取阈值，例如选择标准偏差 $\sigma = \sqrt{M/(n-1) - \mu^2}$，其中均值取 $\mu = M/n$，如果 S 值超出了 $\mu \pm d\sigma$ 的范围就认为异常。变量 $M_1, M_2, \cdots, M_n$ 之间通常不是完全独立的，还需要处理其相关性，此外，采用什么方法得到异常性测量值也需要认真考虑。

统计分析异常检测方法的优势在于所应用的技术方法在统计学中已经比较成熟。其不足在于异常阈值难以确定，阈值设置得偏高会产生过多的误检，偏低则会导致漏检率升高；而且对事件发生的次序不敏感，可能不会检测出由先后发生的几个关联事件组成的入侵行为。此外，对行为的检测结果要么是异常的，要么是正常的，攻击者可以利用这个弱点躲避入侵检测系统的检测。

(2) 贝叶斯推理异常检测

贝叶斯推理异常检测是根据被保护系统当前各种行为特征的测量值进行推理，来判断是否有网络入侵行为发生。系统的特征包括 CPU 利用率、磁盘 I/O 活动数量、系统中的页面出错数量等，分别用异常变量 $A_1, A_2, \cdots, A_n$ 表示。假定变量 A_i 具有两个值，1 表示异常，0 表示正常。I 表示当前系统遭受的入侵攻击。每个异常变量 A_i 的异常可靠性和敏感性分别表示为 $P(A_i=1|I)$ 和 $P(A_i=1|?I)$。如果给出每个 A_i 的值，则可以由贝

叶斯定理得出 I 的可信值：

$$P(I|A_1,A_2,\cdots,A_n)=P(I|A_1,A_2,\cdots,A_n)P(I)/P(A_1,A_2,\cdots,A_n)$$

其中要求给出 I 和?I 的联合率分布。又假定每个测量值 A_i 仅与 I 相关，且同其他测量值 A_j 无关，$i\neq j$，则有：

$$P(A_1,A_2,\cdots,A_n \mid I) = \prod\nolimits_{i=1}^{n} P(A_i \mid I)$$

$$P(A_1,A_2,\cdots,A_n \mid ?I) = \prod\nolimits_{i=1}^{n} P(A_i \mid ?I)$$

从而得到：

$$P(I \mid A_1,A_2,\cdots,A_n)/P(?I \mid A_1,A_2,\cdots,A_n)$$

$$= P(I)\prod\nolimits_{i}^{n} \Big/ \left[P(?I)\prod\nolimits_{i}^{n} P(A_i \mid ?I)\right]$$

这样就可以根据各种异常测量的值、入侵的先验概率以及入侵发生时测量到的各种异常概率计算出受到入侵的概率。必须对各个 A_i 之间的独立性进行处理，才能保证检测的准确性，最常用的一种方法是通过相关性分析，确定各异常变量之间的入侵关系。

(3) 模式预测异常检测

模式预测异常检测方法考虑了事件之间的顺序及其相互联系，认为事件序列都遵循可识别的模式而不是随机的，例如，可以建立和利用时间规则来识别用户正常行为的模式特征，通过归纳学习产生这些规则集，进行不断的修改更新，使之具有较高的预测准确性和可信度。如果规则在大部分情况下是正确的，并且能够成功地运用预测所观察到的数据，规则就具有较高的可信度。

使用模式预测异常检测方法的入侵检测系统通过对用户的行为进行观测记录，归纳产生出一套规则集来构成用户正常行为的轮廓框架。入侵检测系统将当前捕获到的事件序列与规则相匹配，如果根据该规则进行预测所得到的事件与随后实际观察到的事件明显不一致，就说明用户的行为是异常的，入侵检测系统据此检测出入侵行为。

模式预测异常检测方法的优点是能够较好地处理各种用户行为，集中地对相关的安全事件进行考察。缺点是对于不可识别的行为模式会引起误检，因为不可识别的行为模式可能匹配任何规则，而这些行为显然不能与规则的推测结果相一致。

(4) 数据采掘异常检测

将数据采掘技术应用于入侵检测是因为其具有处理大量数据记录的能力。网络流量审计记录的数据量是很大的，特别是在网络中主机数量较多以及网速较快的情况下。数据采掘异常检测技术从各种审计数据或者网络数据流中提取相关的知识信息，这些知识信息是蕴涵在数据之中的，对它们进行归纳总结成为规则、模式等，IDD 算法是所采用的算法之一。入侵检测系统使用这些知识进行网络入侵检测。数据采掘异常检测方法的优势在于处理数据的能力，缺点是系统整体运行效率较低。

(5) 机器学习异常检测

机器学习异常检测方法通过机器学习实现入侵检测，将异常检测问题归结为对离散数据临时序列进行学习来获得个体、系统和网络的行为特征。主要学习方法包括原样记录、监督学习、归纳学习、类比学习等。此外还有基于相似度的实例学习方法(IBL)，该方法通过新的序列相似度计算，将原始数据(例如离散事件流、无序的记录等)转化成可度量

的空间。入侵检测系统使用 IBL 学习技术和一种新的基于序列的分类方法发现异常类型事件,以此检测出入侵行为,其中对阈值的选取由成员分类的概率决定。机器学习异常检测方法的检测速度快,且误报率低。此方法的缺点是对于用户行为发生变化以及单独异常检测的检测效果不理想。

13.3.2 误用检测技术——基于知识的检测

1. 误用检测技术入侵检测系统的基本原理

误用检测技术(misuse detection)也称为基于知识的检测技术或者模式匹配检测技术。它的前提是假设所有的网络攻击行为和方法都具有一定的模式或特征,如果把以往发现的所有网络攻击的特征总结出来并建立一个入侵信息库,那么入侵检测系统可以将当前捕获到的网络行为特征与入侵信息库中的特征信息相比较,如果匹配,则当前行为就被认定为入侵行为。

误用检测技术首先要定义违背安全策略事件的特征,检测主要判别所搜集到的数据特征是否在所搜集到的入侵模式库中出现。这种方法与大部分杀毒软件采用的特征码匹配原理类似。

误用检测就是将搜集到的信息与已知的网络入侵和系统误用模式数据库进行比较,从而发现违背安全策略的行为。该过程可以很简单(如通过字符串匹配以寻找一个简单的条目或指令),也可以很复杂(如利用正规的数学表达式来表示安全状态的变化)。一般来讲,一种进攻模式可以用一个过程(如执行一条指令)或一个输出(如获得权限)来表示。

2. 误用检测技术的评价

误用检测技术有以下优点:

- 检测准确度高;
- 技术相对成熟;
- 便于进行系统防护。

误用检测技术有以下缺点:

- 不能检测出新的入侵行为;
- 完全依赖于入侵特征的有效性;
- 维护特征库的工作量巨大;
- 难以检测来自内部用户的攻击。

3. 误用检测技术的分类

误用检测技术主要可分为以下几种。

(1) 专家系统误用检测

专家系统误用检测方法首先将安全专家的关于网络入侵行为的知识表示成一些类似 If-Then 的规则,并以这些规则为基础建立专家知识库。规则中的 If 部分说明形成网络入侵的必需条件,Then 部分说明发现入侵后要实施的操作。入侵检测系统将网络行为的审计数据事件进行转换,成为包含入侵警告程度的判断事实,然后通过推理引擎进行入侵检测,当 If 中的条件全部满足或者在一定程度上满足时,Then 中的动作就会被执行。

专家系统误用检测需要处理大量的审计数据并且依赖于审计追踪的次序,在目前的

条件下处理速度难以保证。同时,对于各种网络攻击行为知识进行规则化描述的精度有待提高,审计数据有时不能提供足够的检测所需的信息。专家系统只能检测出以往发现过的入侵行为,要检测出新的入侵,必须及时添加新的规则,维护知识库的工作量很大。

(2) 特征分析误用检测

在商业化产品的入侵检测系统中,特征分析技术的运用较多。特征分析误用检测与专家系统误用检测一样,也需要搜集关于网络入侵行为的各种知识。专家系统误用检测由于运行效率的问题,还没有得到普遍的采用,而特征分析更直接地使用各种入侵知识。特征分析误用检测将入侵行为表示成一个事件序列或者转换成某种可以直接在网络数据包审计记录中找到的数据样板,而不进行规则转换,这样可以直接从审计数据中提取相应的数据与之匹配,因此不需要处理大量的数据,从而提高了运行效率。

基于特征分析误用检测技术的系统也必须及时更新知识库,而且对于不同的操作系统,往往需要建立不同的入侵知识记录,建立和维护知识库的工作量都相当大。

(3) 模型推理误用检测

模型推理误用检测方法根据网络入侵行为的特征建立起误用证据模型,入侵检测系统根据模型中的入侵行为特征进行推理,判断当前的用户行为是否是误用行为。模型误用检测方法需要建立攻击剧本数据库、预警器和规划者。每个攻击剧本是一个攻击行为序列,入侵检测系统根据攻击剧本的子集来推断系统当前是否受到入侵。根据当前的活动模型,预警器产生下一步行为,规划者负责判断所假设的行为如何反应在审计追踪数据上,以及如何将假设的行为与系统相关的审计追踪进行匹配。各个攻击剧本的证据会逐渐增加,活动模型组也会被更新,证据推理分析功能可以更新活动模型列表中的各攻击剧本出现的概率,根据攻击剧本的概率来推断检测入侵。这种方法的优势在于有数学中的未确定推理理论作为基础,可以用模型证据来推理专家系统不容易处理的未确定的中间结论,而且还能够减少审计数据量;不足之处是增加了创建入侵检测模型的系统开销。此外,这种方法也只能检测出已知的入侵行为,需要对数据库进行不断地扩充。

(4) 条件概率误用检测

条件概率误用检测方法将网络入侵方式看作一个事件序列,根据所观测到的各种网络事件的发生情况来推测入侵行为的发生。条件概率误用检测方法应用贝叶斯定理对入侵进行推理检测,原理如下:

事件序列表示为 ES,先验概率为 $P(\mathrm{Intrusion})$,后验概率为 $P(\mathrm{ES}|\mathrm{Intrusion})$,事件出现的概率为 $P(\mathrm{ES})$,则

$$P(\mathrm{Intrusion} \mid \mathrm{ES}) = P(\mathrm{ES} \mid \mathrm{Intrusion})P(\mathrm{Intrusion})/P(\mathrm{ES})$$

其中,先验概率 $P(\mathrm{Intrusion})$由网络安全专家给出,对以往网络入侵数据进行统计处理可以得出后验概论 $P(\mathrm{ES}|\mathrm{Intrusion})$和 $P(\mathrm{ES}|?\mathrm{Intrusion})$,于是可以计算出:

$$P(\mathrm{ES}) = (P(\mathrm{ES} \mid \mathrm{Intrusion}) - P(\mathrm{ES} \mid ?\mathrm{Intrusion}))P(\mathrm{Intrusion}) + P(\mathrm{ES} \mid ?\mathrm{Intrusion})$$

因此可以通过对事件序列的观测推算出 $P(\mathrm{ES}|\mathrm{Intrusion}|\mathrm{ES})$。条件概率误用检测的缺点是先验概率难以给出,而且难以确定事件的独立性。

(5) 键盘监控误用检测

键盘监控误用检测方法假设每种网络入侵行为都具有特定的击键序列模式,入侵检

测系统监视各个用户的击键模式，并将该模式与已有的入侵击键模式相匹配，如果匹配成功就认为是网络入侵行为。这种方法的不足之处是如果操作系统没有提供相应的支持，则缺少可靠的方法来捕获用户的击键行为，可能存在多种击键方式表示同一种攻击的情况，而且不能对击键进行语义分析，攻击者使用命令的各种别名就很容易欺骗这种技术。此外，因为这种技术仅分析击键行为，所以对于那些利用程序进行自动攻击的行为无法检测。

13.3.3　异常检测技术和误用检测技术的比较

无论哪种入侵检测技术都需要搜集总结有关网络入侵行为的各种知识，或者系统及其用户的各种行为的知识。基于异常检测技术的入侵检测系统如果想检测到所有的网络入侵行为，必须掌握被保护系统已知行为和预期行为的所有信息，这一点实际上无法做到，因此入侵检测系统必须不断地学习并更新已有的行为轮廓。对于基于误用检测技术的入侵检测系统而言，只有拥有所有可能的入侵行为的先验知识，而且必须能识别各种入侵行为的过程细节或者每种入侵行为的特征模式，才能检测到所有的入侵行为，而这种情况也是不存在的，该类入侵检测系统只能检测出已有的入侵模式，必须不断地对新出现的入侵行为进行总结和归纳。

在入侵检测系统的配置方面，基于异常检测技术的入侵检测系统通常比基于误用检测技术的入侵检测系统所做的工作要少很多，因为异常检测需要对系统和用户的行为轮廓进行不断的学习更新，需要大量的数据分析处理工作，要求管理员能够总结出被保护系统的所有正常行为状态，对系统的已知和期望行为进行全面的分析，因此配置难度相对较大。但是，有些基于误用检测技术的入侵检测系统允许管理员对入侵特征数据库进行修改，甚至允许管理员自己根据所发现的攻击行为创建新的网络入侵特征规则记录，这种入侵检测系统在系统配置方面的工作量会显著增加。

基于异常检测技术的入侵检测系统所输出的检测结果，通常是在对实际行为与行为轮廓进行异常分析等相关处理后得出的，这类入侵检测系统的检测报告通常会比基于误用检测技术的入侵检测系统具有更多的数据量，因为任何超出行为轮廓范围的事件都将被检测出来并写入报告中。而大多数基于误用检测技术的入侵检测系统，是将当前行为模式与已有行为模式进行匹配后产生检测结论，其输出内容是列举出入侵行为的类型和名称，以及提供相应的处理建议。

13.3.4　其他入侵检测技术的研究

入侵检测系统的研究方向之一是将各个领域的研究成果应用于入侵检测中，以形成更高效、更为智能化的检测算法，提高入侵检测的应用价值。目前研究的重点有遗传算法和免疫技术等。从提高入侵检测分析效率角度，针对高层协议的状态分析检测技术也是研究的重点。

1. 遗传算法

遗传算法的基本原理是首先定义一组入侵检测指令集，这些指令用于检测出正常或者异常的行为。指令中包含若干字符串，所有的指令在定义初期的检测能力都很有限，入

侵检测系统对这些指令逐步地进行训练，促使指令中的字符串片段发生重组，以生成新的字符串指令。再从新的指令中经过测试筛选出检测能力最强的部分指令，对它们进行下一轮的训练。如此反复，使检测指令的检测能力不断提高，这个过程如同生物学中的遗传进化过程。直到指令的检测能力不会有明显的提高，训练过程即可结束，此时这些指令已经具有一定的检测能力，入侵检测系统可以使用它们进行网络入侵检测。目前对遗传算法的研究还处于试验阶段。

2. 免疫技术

免疫技术应用了生物医学中的免疫系统原理。处于网络环境中的主机之所以受到入侵，是因为主机系统本身以及所运行的应用程序存在着各种脆弱性因素，网络攻击者正是利用这些漏洞来侵入到主机系统中的；在生物系统中同样存在各种脆弱性因素，因此会受到病毒、病菌的攻击。而生物体拥有免疫系统来负责检测和抵御入侵，免疫机制包括特异性免疫和非特异性免疫。特异性免疫针对于特定的某种病毒，非特异性免疫可用于检测和抵制以前从未体验过的入侵类型。入侵检测免疫技术受免疫系统原理的启发，通过学习分析已有行为的样本来获得识别不符合常规行为的能力。

3. 基于应用协议状态的跟踪型入侵检测技术

目前入侵检测主要根据协议内容，进行匹配性检测。从状态跟踪上还仅限于 tcp/ip 层数据包状态的跟踪。而对于应用协议来说，高层应用协议也具有大量的不同状态，为了检测到只会在某种协议状态下才存在的攻击而去将攻击特征匹配所有状态下的数据显然是浪费的，同时也降低了准确性和效率。因此，跟踪型入侵检测技术实现对高层应用协议的状态跟踪，建立高层应用协议状态机。跟踪协议状态的变化，对每个状态下的数据包仅分析该状态下存在的入侵行为。这样的分析方法在确保不会出现入侵检测欺骗行为的同时，还可以解决针对入侵检测拒绝服务攻击造成的海量报警问题。分状态的攻击特征匹配也降低了单个数据的分析时间，提高了分析效率，提高了分析带宽。

13.4　入侵检测系统的设置

网络安全需要各个安全设备的协同工作和正确的设置，因此，入侵检测系统在设置时需要对整个网络有一个全面的了解，保证自身环境的正确性和安全性。网络安全的实际需求对于入侵检测的工作方式和检测位置都有十分重要的影响，只有在了解和掌握这些实际需求的情况下，才能正确地设计入侵检测系统的网络拓扑，并对入侵检测系统进行正确的配置。

入侵检测系统是网络安全防御系统的重要组成部分。入侵检测系统的设置影响着入侵检测系统在整个网络安全防御体系中的地位和重要程度。目前大部分的入侵检测技术都需要对网络数据流进行大量的分析运算，在高速网络中，一个不经过配置的入侵检测设备，在不进行筛选和过滤的情况下，无法很好地完成对受保护网络的有效检测。

由于入侵检测系统位于网络体系结构中的高层部分，因此，高层应用的多样性也就导致了入侵检测系统分析的复杂性和对计算资源的高需求。如何根据受保护网络的拓扑结

构和运行情况对入侵检测设备进行合理的优化配置，是保证入侵检测系统有效运行的关键。

入侵检测系统的设置主要分为以下几个基本的步骤：

① 确定入侵检测需求；

② 设计入侵检测系统在网络中的拓扑位置；

③ 配置入侵检测系统；

④ 入侵检测系统磨合；

⑤ 入侵检测系统的使用及自调节。

这些步骤的操作流程如图 13-2 所示。

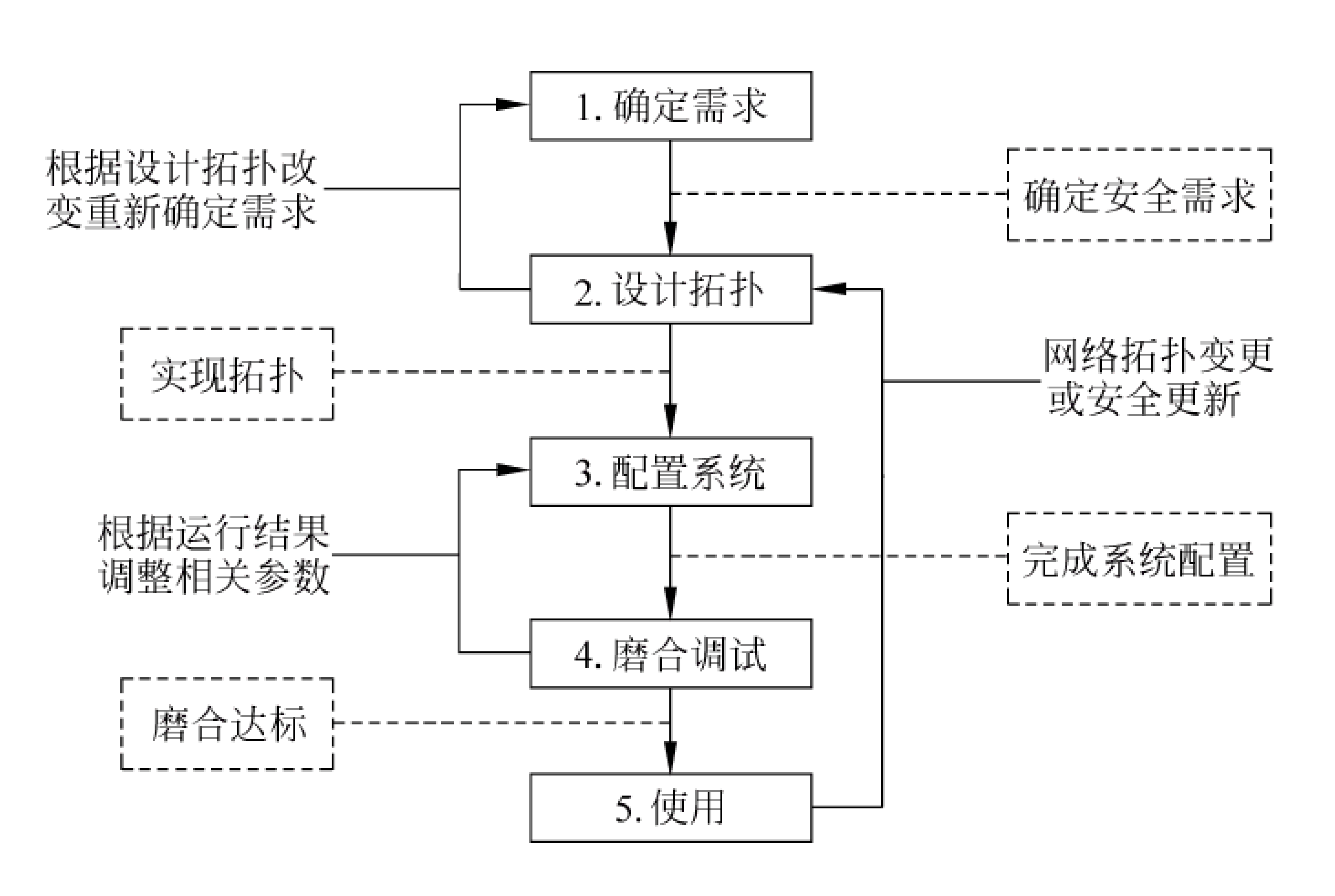


图 13-2　入侵检测系统设置流程图

入侵检测系统的设置需要经过多次的反复磨合，才能够达到与本保护网络有效结合的目的。在图 13-2 中可以看到，在设置的过程中要进行多次的回溯，而在这几次回溯中，第 3、4 步的回溯过程会重复多次，通过不断地调整入侵检测系统的检测配置，将误报警率和漏报警率降到最低，使得入侵检测系统能够在最佳状态下进行检测分析。而在使用中，随着网络整体结构的改变（包括增加新的应用或服务器、检测方式更新等），入侵检测系统的设置也要相应地进行修改，以保证能够适应新的变化。

通过以上的设置步骤，入侵检测系统才能够很好地与被保护网络相结合，实现对网络的有效监控和分析。

13.5　入侵检测系统的部署

入侵检测系统有不同的部署方式和特点。根据所掌握的网络检测和安全需求，选取各种类型的入侵检测系统。将多种入侵检测系统按照预定的计划进行部署，确保每个入侵检测系统都能够在相应部署点上发挥作用，共同防护，保障网络的安全运行。

部署工作包括对网络入侵检测和主机入侵检测等类型入侵检测系统的部署规划。同

时，根据主动防御网络的需求，还需要对入侵检测系统的报警方式进行部署和规划。

13.5.1　基于网络入侵检测系统的部署

基于网络的入侵检测系统可以在网络的多个位置进行部署。这里的部署主要指对网络入侵检测器的部署。根据检测器部署位置的不同，入侵检测系统具有不同的工作特点。用户需要根据自己的网络环境以及安全需求进行网络部署，以达到预定的网络安全需求。总体来说，入侵检测的部署点可以划分为 4 个位置：①DMZ 区；②外网入口；③内网主干；④关键子网。如图 13-3 所示。

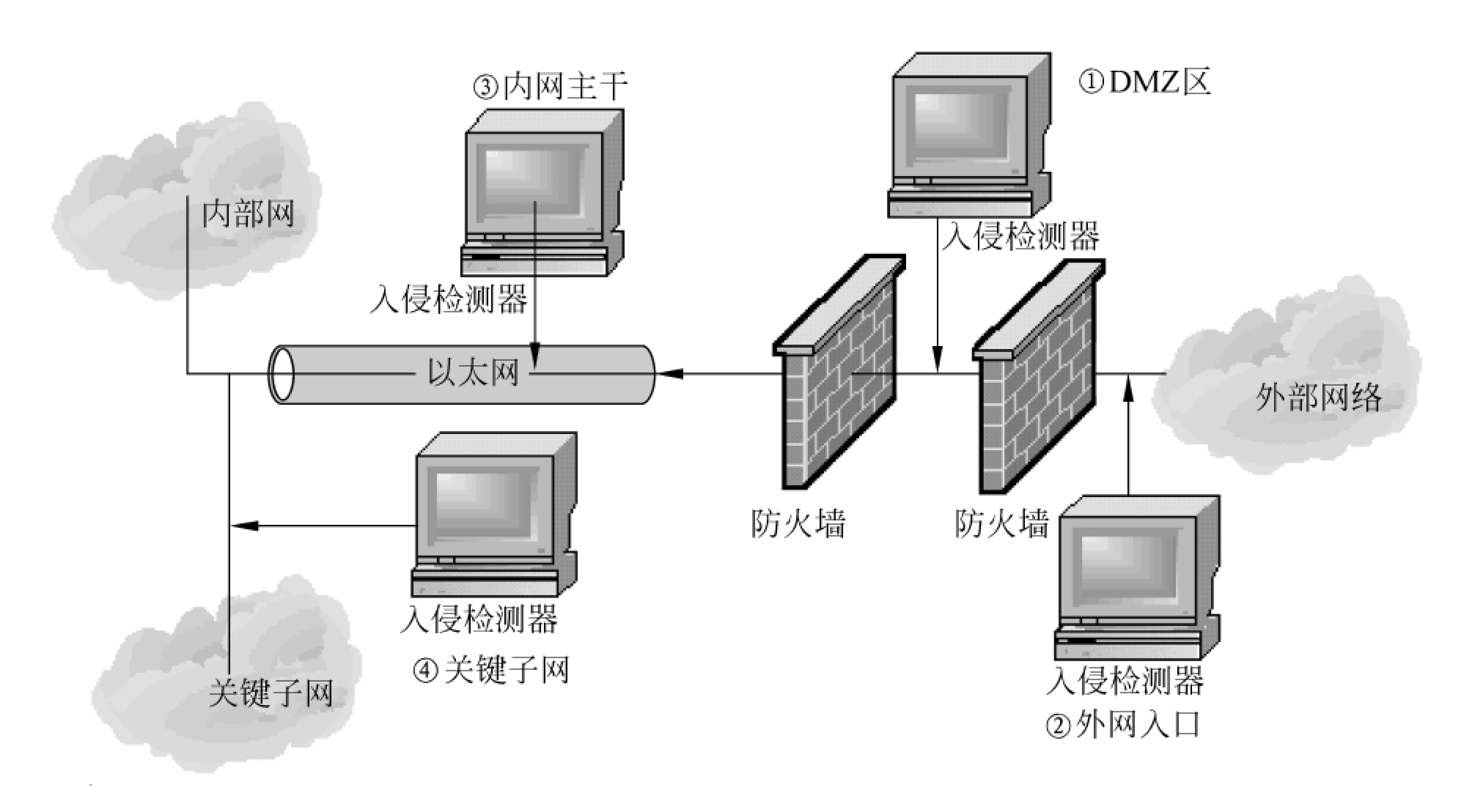


图 13-3　入侵检测系统部署位置图

1. DMZ 区

DMZ 区部署点在 DMZ 区的总口上，这是入侵检测器最常见的部署位置。在这里入侵检测器可以检测到所有针对用户向外提供服务的服务器进行攻击的行为。对于用户来说，防止对外服务的服务器受到攻击是最为重要的。由于 DMZ 区中的各个服务器提供的服务有限，所以针对这些对外提供的服务进行入侵检测，可以使入侵检测器发挥最大的优势，对进出的网络数据进行分析。由于 DMZ 区中的服务器是外网可见的，因此，在这里的入侵检测也是最为需要的。

在该部署点进行入侵检测有以下优点：

- 检测来自外部的攻击，这些攻击已经渗入过第一层防御体系；
- 可以容易地检测网络防火墙的性能并找到配置策略中的问题；
- DMZ 区通常放置的是对内外提供服务的重要的服务设备，因此，所检测的对象集中于关键的服务设备；
- 即使进入的攻击行为不可识别，入侵检测系统经过正确的配置也可以从被攻击主机的反馈中获得受到攻击的信息。

2. 外网入口

外网入口部署点位于防火墙之前，入侵检测器在这个部署点可以检测所有进出防火墙外网口的数据。在这个位置上，入侵检测器可以检测到所有来自外部网络的可能的攻击行为并进行记录，这些攻击包括对内部服务器的攻击、对防火墙本身的攻击以及内网机器不正常的数据通信行为。

由于该部署点在防火墙之前，因此入侵检测器将处理所有的进出数据。这种方式虽然对整体入侵行为记录有帮助，但由于入侵检测器本身性能上的局限，该部署点的入侵检测器目前的效果并不理想，同时对于进行 NAT 的内部网来说，入侵检测器不能定位攻击的源或目的地址，系统管理员在处理攻击行为上存在一定的难度。

在该部署点进行入侵检测有以下优点：

- 可以对针对目标网络的攻击进行计数，并记录最为原始的攻击数据包；
- 可以记录针对目标网络的攻击类型。

3. 内网主干

内网主干部署点是最常用的部署位置，在这里入侵检测器主要检测内网流出和经过防火墙过滤后流入内网的网络数据。在这个位置，入侵检测器可以检测所有通过防火墙进入的攻击以及内部网向外部的不正常操作，并且可以准确地定位攻击的源和目的，方便系统管理员进行针对性的网络管理。

由于防火墙的过滤作用，防火墙已经根据规则要求抛弃了大量的非法数据包。这样就降低了通过入侵检测器的数据流量，使得入侵检测器能够更有效地工作。当然，由于入侵检测器在防火墙的内部，防火墙已经根据规则要求阻断了部分攻击，所以入侵检测器并不能记录下所有可能的入侵行为。

在该部署点进行入侵检测有以下优点：

- 检测大量的网络通信提高了检测攻击的识别可能；
- 检测内网可信用户的越权行为；
- 实现对内部网络信息的检测。

4. 关键子网

在内部网中，总有一些子网因为存在关键性数据和服务，需要更严格的管理，比如资产管理子网、财务子网、员工档案子网等，这些子网是整个网络系统中的关键子网。通过对这些子网进行安全检测，可以检测到来自内部以及外部的所有不正常的网络行为，这样可以有效地保护关键的网络不会被外部或没有权限的内部用户侵入，造成关键数据泄露或丢失。由于关键子网位于内网的内部，因此流量相对要小一些，可以保证入侵检测器的有效检测。

在该部署点进行入侵检测具有以下优点：

- 集中资源用于检测针对关键系统和资源的来自企业内外部的攻击；
- 将有限的资源进行有效部署，获取最高的使用价值。

13.5.2　基于主机入侵检测系统的部署

在基于网络的入侵检测系统部署并配置完成后，基于主机的入侵检测系统的部署可以给系统提供高级别的保护。但是，将基于主机的入侵检测系统安装在企业中的每一个主机上是一种相当大的时间和资金的浪费，同时每一台主机都需要根据自身的情况进行特别的安装和设置，相关的日志和升级维护是巨大的。

因此，基于主机的入侵检测系统主要安装在关键主机上，这样可以减少规划部署的花费，使管理的精力集中在最重要最需要保护的主机上。同时，为了便于对基于主机的入侵检测系统的检测结果进行及时检查，需要对系统产生的日志进行集中。通过进行集中的分析、整理和显示，可以大大减少对网络安全系统日常维护的复杂性和难度。由于基于主机的入侵检测系统本身需要占用服务器的计算和存储资源，因此，要根据服务器本身的空闲负载能力选取不同类型的入侵检测系统并进行专门的配置。如对于高负载的网络服务器，为了不影响网络服务的能力，需要针对所提供的服务进行专门的配置，选择与所提供服务相关的策略进行加载。对于负载过大的服务器，可以选择非实时的日志分析类型入侵检测器，通过二次审计对服务器状态进行检测。

13.5.3　报警策略

入侵检测系统在检测到入侵行为的时候，需要报警并进行相应的反应。如何报警和选取什么样的报警，需要根据整个网络的环境和安全的需求进行确定。

网络安全需求不同，入侵检测报警也就存在不同的方式。如对于一般性服务的企业，报警主要集中在已知的有威胁的攻击行为上；关键性服务企业则需要将尽可能多的报警进行记录并对部分认定的报警进行实时的反馈。不同的报警方式对网络相关的设备有着不同的要求。由于报警的形式很多，大部分都需要其他网络设备和服务的协助，因此只有保证相关的设备和服务可以和入侵检测系统正确地通信，才可以保证报警信息的及时送达。这就要求入侵检测系统存在与其他设备互动的接口。通常这个接口是安全防御系统中的关键设备，因此，需要保证这个互动的接口与目标网络物理隔绝，以防止入侵检测系统本身受到攻击和检测受到不必要的干扰。

13.6　入侵检测系统的优点与局限性

入侵检测系统是企业安全防御系统中的重要部件，但入侵检测系统并不是万能的。入侵检测对于部分事件可以处理得很好，但对于另一些情况则无能为力。只有充分了解入侵检测系统的优点和局限性，才能对入侵检测系统有一个准确的定位，以便将入侵检测系统有效地应用在安全防御系统中，最大限度地发挥它的安全防御功能。

13.6.1　入侵检测系统的优点

入侵检测系统作为一个迅速崛起并受到广泛承认的安全组件，有着很多方面的安全

优势：

- 可以检测和分析系统事件以及用户的行为；
- 可以测试系统设置的安全状态；
- 以系统的安全状态为基础，跟踪任何对系统安全的修改操作；
- 通过模式识别等技术从通信行为中检测出已知的攻击行为；
- 可以对网络通信行为进行统计，并进行检测分析；
- 管理操作系统认证和日志机制并对产生的数据进行分析处理；
- 在检测到攻击的时候，通过适当的方式进行适当的报警处理；
- 通过对分析引擎的配置对网络的安全进行评估和监督；
- 允许非安全领域的管理人员对重要的安全事件进行有效的处理。

13.6.2　入侵检测系统的局限性

入侵检测系统只能对网络行为进行安全审计，从入侵检测系统的定位可以看出，入侵检测系统存在以下缺陷。

（1）入侵检测系统无法弥补安全防御系统中的安全缺陷和漏洞。这些安全缺陷和漏洞包括其他安全设备的错误配置造成的安全漏洞，以及安全设备本身的实现造成的安全缺陷。入侵检测系统可以通过审计报警对这些可能的安全漏洞进行揭示和定位，但却不能主动对这些漏洞进行弥补，而这些报警信息只有通过人为的补救处理才具有意义。

（2）对于高负载的网络或主机，很难实现对网络入侵的实时检测、报警和迅速地进行攻击响应。同时，对于高负载的环境，如果没有采用代价较大的负载均衡措施，入侵检测系统会存在较大的分析遗漏，容易造成较大的漏报警率。

（3）基于知识的入侵检测系统很难检测到未知的攻击行为，也就是说，检测具有一定的后滞性，而对于已知的报警，一些没有明显特征的攻击行为也很难检测到，或需要付出提高误报警率的代价才能够正确检测。而基于行为特征的入侵检测系统只能在一定程度上检测到新的攻击行为，但一般很难给新的攻击定性，提供给系统管理员的处理信息较少，很难进行进一步的防护处理。

（4）入侵检测系统的主动防御功能和联动防御功能会对网络的行为产生影响，同样也会成为攻击者的目标，实现以入侵检测系统过敏自主防御为基础的攻击。通过发送伪造的数据，触发入侵检测系统的主动防御响应，对可信连接进行阻断，造成拒绝服务攻击。在目前的技术条件下，对于网络的主动防御的设置要十分慎重，防止出现利用主动防御系统进行网络攻击的情况。

（5）入侵检测系统无法单独防止攻击行为的渗透，只能调整相关网络设备的参数或人为地进行处理。由于入侵检测技术不可避免地存在着大量的误报情况，因此进行自动防御会造成对可信连接的影响。目前的入侵检测系统在实质性安全防御方面，还是要以人为修正为主，即使是对可确定入侵的自动阻断行为，建议也要经过人为干预，防止可能的过敏防御。

（6）网络入侵检测系统在纯交换环境下无法正常工作，只有对交换环境进行一定的处理，利用镜像等技术，网络入侵检测系统才能对镜像的数据进行分析处理。因此，在交

换环境中,进行各个方向的检测分析将非常困难并且代价较大。

(7) 入侵检测系统主要是对网络行为进行分析检测,不能修正信息资源中存在的安全问题。

13.7　本章小结

入侵检测是从计算机网络或计算机系统中的若干关键点搜集信息并对其进行分析,从中发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象的一种机制。

入侵检测系统使用入侵检测技术对网络与其上的系统进行监视,并根据监视结果进行不同的安全动作,最大限度地降低可能的入侵危害。

入侵检测系统主要由 4 个部分组成:事件产生器、事件分析器、响应单元和事件数据库。

入侵检测系统根据信息来源与类型可以分为基于主机和基于网络两大类。入侵防护系统采用入侵检测技术,是一种基于高层应用防护的网络安全防护设备。

异常检测技术也称为基于行为的检测技术,是指根据用户的行为和系统资源的使用状况判断是否存在网络入侵。

误用检测技术也称为基于知识的检测技术或者模式匹配检测技术,它通过对实际行为和数据的特征匹配判断是否存在已知的网络入侵行为。

入侵检测系统可以部署在 4 个位置上:DMZ 区、外网入口、内网主干、关键子网。

要根据目标网络的具体情况以及企业的安全需求对入侵检测系统进行适当的配置,保证入侵检测系统正常有效地运行。

在进行入侵检测系统运行管理时,需要保证及时处理系统输出;及时更新系统检测行为,适应网络不断变化的需求;同时注意对保存的日志信息的进一步分析和处理。通过认真的日常管理,保证入侵检测系统发挥最大的安全保障作用。

习　　题

1. 什么叫做入侵检测系统?
2. 简单地介绍一下入侵检测系统的基本结构。
3. 简述 NIDS 的基本原理。
4. HIDS 与 NIDS 相比有哪些优势和不足?
5. 试分析基于主机网络连接检测的 IDS 与基于网络的 IDS 的基本区别。
6. 简述异常检测技术的基本原理。
7. 试比较异常检测技术和误用检测技术各有哪些优势和不足。
8. 以一种检测算法为例,简单说明基于误用检测技术的 IDS 的工作过程。
9. 简单描述入侵检测系统的配置流程。
10. 参照你所了解的局域网,对网络信息进行搜集,制定一个入侵检测系统的配置计

划，画出配置拓扑图。

11. 结合所在的局域网，制定一个入侵检测系统的运行管理计划。

12. 简述入侵检测系统的优缺点。

13. 入侵防护是入侵检测的发展方向吗？入侵防护会不会完全取代入侵检测？请阐述自己的观点。

第14章 恶意代码与计算机病毒的防治

本章要点：

- 恶意代码的概念和分类；
- 计算机病毒的概念和结构；
- 恶意代码与计算机病毒防治的技术、部署、管理和软件。

14.1 恶意代码

14.1.1 恶意代码的概念

代码是指计算机程序代码，可以被执行完成特定功能。任何事物都有正反两面，人类发明的所有工具既可造福也可作孽，这完全取决于使用工具的人。计算机程序也不例外，在善良的软件工程师们编写了大量的有用软件(操作系统、应用系统、数据库系统等)的同时，黑客们却在编写着扰乱社会和他人，甚至起着破坏作用的计算机程序，这就是恶意代码。

14.1.2 恶意代码的分类

恶意代码可以按照两种分类标准，从两个角度进行直交分类。一种分类标准是，恶意代码是否需要宿主，即特定的应用程序、工具程序或系统程序。需要宿主的恶意代码具有依附性，不能脱离宿主而独立运行；不需要宿主的恶意代码具有独立性，可不依赖宿主而独立运行。另一种分类标准是，恶意代码是否能够自我复制。不能自我复制的恶意代码是不感染的；能够自我复制的恶意代码是可感染的。由此，可以得出以下4大类恶意代码(见表14-1)：

- 不感染的依附性恶意代码；
- 不感染的独立性恶意代码；
- 可感染的依附性恶意代码；
- 可感染的独立性恶意代码。

表 14-1 恶意代码的分类方法

分类标准	需要宿主	不需要宿主
不能自我复制	不感染的依附性恶意代码	不感染的独立性恶意代码
能够自我复制	可感染的依附性恶意代码	可感染的独立性恶意代码

目前发现并命名的主要恶意代码按上述分类方法的分类结果如表 14-2 所示。

表 14-2 恶意代码的分类实例

类别	实例
不感染的依附性恶意代码	特洛伊木马(Trojan horse) 逻辑炸弹(logic bomb) 后门(backdoor)或陷门(trapdoor)
不感染的独立性恶意代码	点滴器(dropper) 繁殖器(generator) 恶作剧(hoax)
可感染的依附性恶意代码	病毒(virus)
可感染的独立性恶意代码	蠕虫(worm) 细菌(germ)

1. 不感染的依附性恶意代码

(1) 特洛伊木马

关于特洛伊木马(Trojan horse)有一个典故。大约在公元前 12 世纪,因为特洛伊王子劫持了斯巴达国王梅尼拉斯的妻子海伦,希腊向特洛伊城宣战。战争持续了 10 年,特洛伊城非常坚固,希腊军队无法攻入。后来,希腊军队撤退,在特洛伊城外留下了很多巨大的木马。特洛伊城的军民以为这是希腊军队留给他们的礼物,就将这些木马运进城内。没想到木马中隐藏有希腊最好的战士,到了夜晚,这些希腊士兵在奥迪塞斯的带领下打开特洛伊城的城门,于是希腊军队夺下了特洛伊城。据说"小心希腊人的礼物"这一谚语也是出于这个典故。

在计算机领域,特洛伊木马是一段吸引人而不为人警惕的程序,但它们可以执行某些秘密任务。大多数安全专家统一认可的定义是:"特洛伊木马是一段能实现有用的或必需的功能的程序,但是同时还完成一些不为人知的功能,这些额外的功能往往是有害的。"

这个定义中有 3 点需要进一步解释:

第一,"有用的或必需的功能的程序"只是诱饵,就像典故里的特洛伊木马,表面看上去很美但实际上暗藏危机。

第二,"不为人知的功能"定义了其欺骗性,是危机所在之处,为几乎所有的特洛伊木马所必备的特点。

第三,"往往是有害的"定义了其恶意性,恶意企图包括:(1)试图访问未授权资源(如盗取口令、个人隐私或企业机密);(2)试图阻止正常访问(如拒绝服务攻击);(3)试图更改或破坏数据和系统(如删除文件、创建后门等)。

特洛伊木马一般没有自我复制的机制，所以不会自动复制自身。电子新闻组和电子邮件是特洛伊木马的主要传播途径。特洛伊木马的欺骗性是其得以传播的根本原因。特洛伊木马经常伪装成游戏软件、搞笑程序、屏保、非法软件、色情资料等，上传到电子新闻组或通过电子邮件直接传播，很容易被不知情的用户接收和继续传播。

1997 年 4 月，一伙人开发出一个名叫 AOL4FREE.COM 的特洛伊木马，声称可以免费访问 AOL，但它却损坏了执行它的机器硬盘。

(2) 逻辑炸弹

逻辑炸弹(logic bomb)是一段具有破坏性的代码，事先预置于较大的程序中，等待某扳机事件发生触发其破坏行为。扳机事件可以是特殊日期，也可以是指定事件。逻辑炸弹往往被那些有怨恨的职员利用，他们希望在离开公司后，通过启动逻辑炸弹来损伤公司利益。一旦逻辑炸弹被触发，就会造成数据或文件的改变或删除、计算机死机等破坏性事件。

一个著名的例子是美国马里兰州某县的图书馆系统，开发该系统的承包商在系统中插入了一个逻辑炸弹，如果承包商在规定日期得不到全部酬金，它将在该日期使整个系统瘫痪。当图书馆因系统响应时间过长准备扣留最后酬金时，承包商指出了逻辑炸弹的存在，并威胁如果酬金不到位的话就会让它爆炸。

(3) 后门或陷门

后门(backdoor)或陷门(trapdoor)是进入系统或程序的一个秘密入口，它能够通过识别某种特定的输入序列或特定账户，使访问者绕过访问的安全检查，直接获得访问权利，并且通常高于普通用户的特权。多年来，程序员为了调试和测试程序一直合法地使用后门，但当程序员或他所在的公司另有企图时，后门就变成了一种威胁。

2 不感染的独立性恶意代码

(1) 点滴器

点滴器(dropper)是为传送和安装其他恶意代码而设计的程序，它本身不具有直接的感染性和破坏性。点滴器专门对抗反病毒检测，使用了加密手段，以阻止反病毒程序发现它们。当特定事件出现时，它便启动，将自身包含的恶意代码释放出来。

(2) 繁殖器

繁殖器(generator)是为制造恶意代码而设计的程序，通过这个程序，只要简单地从菜单中选择你想要的功能，就可以制造恶意代码，不需要任何程序设计能力。事实上，它只是把某些已经设计好的恶意代码模块按照使用者的选择组合起来而已，没有任何创造新恶意代码的能力。因此，检测由繁殖器产生的任何病毒都比较容易，只要通过搜索一个字符串，每种组合都可以被发现。繁殖器的典型例子是 VCL(virus creation laboratory)。

(3) 恶作剧

恶作剧(hoax)是为欺骗使用者而设计的程序，它侮辱使用者或让其做出不明智的举动。恶作剧通过“心理破坏”达到“现实破坏”。例如，UltraCool 声称“如果不按退出按钮的话，一个低水平的硬盘格式化会在 27 秒内完成”，然而如果一直用鼠标按住退出按钮的话，直到计时到 0 时，便会出现一个“只是玩笑”的信息。这只是愚弄而已，严重的问题是

有些恶作剧会让受骗者相信他的数据正在丢失或系统已经损坏需要重新安装，惊慌失措的受骗者可能会做出不明智的操作，如设法恢复丢失的数据或阻止数据再次丢失，或进行系统重新安装而致使数据丢失甚至无法进入系统，从而导致真正的破坏。

3. 可感染的依附性恶意代码

计算机病毒(virus)是一段附着在其他程序上的可以进行自我繁殖的代码。由此可见，计算机病毒是既有依附性，又有感染性。

由于绝大多数恶意代码都或多或少地具有计算机病毒的特征，因此在下一节中专门论述计算机病毒，这里不多做解释。

4. 可感染的独立性恶意代码

(1) 蠕虫

计算机蠕虫(worm)是一种通过计算机网络能够自我复制和扩散的程序。蠕虫与病毒的区别在于“附着”。蠕虫不需要宿主，不会与其他特定程序混合。因此，与病毒感染特定目标程序不同，蠕虫感染的是系统环境(如操作系统或邮件系统)。

蠕虫利用一些网络工具复制和传播自身，其中包括：

- 电子邮件　蠕虫会把自身的副本邮寄到其他系统中；
- 远程执行　蠕虫能够执行在其他系统中的副本；
- 远程登录　蠕虫能够像用户一样登录到远程系统中，然后使用系统命令将其自身从一个系统复制到另一个系统中。

上述方式的递归过程，即新感染系统采取同样的上述方式进行复制和传播，使得蠕虫传播非常迅速。蠕虫可以大量地消耗计算机时间和网络通信带宽，导致整个计算机系统及其网络的崩溃，成为拒绝服务攻击的工具。

Carey Nachenberg 建议对蠕虫进行如下分类。

根据传播方式可分为几种。

- 电子邮件蠕虫(E-mail worm)　通过电子邮件传播；
- 任意协议蠕虫(arbitrary protocol worm)　通过电子邮件以外的其他网络协议传播。

根据启动方式可分为几种。

- 自动启动蠕虫(self-launching worm)　不需要与受害者交互而自动执行，如 morris worm；
- 用户启动蠕虫(user-launched worm)　必须由使用者来执行，因此需要一定的伪装，如 CHRISTMA EXEC；
- 混合启动蠕虫(hybrid-launch worm)　包含上述两种启动方式。

(2) 细菌

计算机细菌(germ)是一种在计算机系统中不断复制自己的程序。一个典型的细菌是在多任务系统中生成它的两个副本，然后同时执行这两个副本，这一过程递归循环，迅速以指数形式膨胀，最终会占用全部的处理器时间和内存或磁盘空间，从而导致计算资源耗尽无法为用户提供服务。细菌通常发生在多用户系统和网络环境中，目的就是占用所

有的资源。

上述分类是为了从概念上把握恶意代码的主要特征，便于理解和研究。随着恶意代码的不断进化，实际中的许多恶意代码同时具有多种特征，这样可以具有更大的威胁性。最典型的是蠕虫病毒，它是蠕虫和病毒的混合体，同时具有蠕虫和病毒的特征。

14.2 计算机病毒

严格地从概念上讲，计算机病毒是恶意代码的一种，即可感染的依附性恶意代码，这是纯粹意义上的计算机病毒概念。实际上，目前发现的恶意代码几乎都是混合型的计算机病毒，即除了具有纯粹意义上的病毒特征外，还带有其他类型恶意代码的特征。蠕虫病毒就是最典型和最常见的恶意代码，它是蠕虫和病毒的混合体。加之“病毒”一词非常形象且很具感染力，因此，媒体、杂志，包括很多专业文章和书籍都喜欢用“计算机病毒”来指学术上的恶意代码。在这个意义上讲，“计算机病毒”一词就不仅限于纯粹的计算机病毒，而是指混合型的计算机病毒。

本节在概念论述上给出纯粹意义上的计算机病毒的定义，在技术说明上则涉及范围更广的混合型计算机病毒。

14.2.1 计算机病毒的概念

“计算机病毒”最早是由美国计算机病毒研究专家 Fred Cohen 博士正式提出的。“病毒”一词来源于生物学，因为计算机病毒与生物病毒在很多方面有着相似之处。

Fred Cohen 博士对计算机病毒的定义是：“病毒是一种靠修改其他程序来插入或进行自身复制，从而感染其他程序的一段程序。”这一定义作为标准已被普遍地接受。

在《中华人民共和国计算机信息系统安全保护条例》中的定义为：“计算机病毒是指编制者在计算机程序中插入的破坏计算机功能或者数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。”

计算机病毒（简称病毒）具有以下特征：

（1）传染性

病毒通过各种渠道从已被感染的计算机扩散到未被感染的计算机。病毒程序一旦进入计算机并得以执行，就会寻找符合感染条件的目标，将其感染，达到自我繁殖的目的。所谓“感染”，就是病毒将自身嵌入到合法程序的指令序列中，致使执行合法程序的操作会招致病毒程序的共同执行或以病毒程序的执行取而代之。因此，只要一台计算机染上病毒，如不及时处理，那么病毒会在这台机子上迅速扩散，其中的大量文件（一般是可执行文件）就会被感染。而被感染的文件又成了新的传染源，再与其他机器进行数据交换或通过网络接触，病毒会继续传染。病毒通过各种可能的渠道，如可移动存储介质（如软盘）、计算机网络去传染其他计算机。往往曾在一台染毒的计算机上用过的软盘已感染上了病毒，与这台机器联网的其他计算机也许也被染上病毒了。传染性是病毒的基本特征。

（2）隐蔽性

病毒一般是具有很高编程技巧的、短小精悍的一段代码，躲在合法程序当中。如果不

经过代码分析，病毒程序与正常程序是不容易区别开来的。这是病毒程序的隐蔽性。在没有防护措施的情况下，病毒程序取得系统控制权后，可以在很短的时间里传染大量其他程序，而且计算机系统通常仍能正常运行，用户不会感到任何异常，好像在计算机内不曾发生过什么。这是病毒传染的隐蔽性。

（3）潜伏性

病毒进入系统之后一般不会马上发作，可以在几周或者几个月甚至几年内隐藏在合法程序中，默默地进行传染扩散而不被人发现，潜伏性越好，在系统中的存在时间就会越长，传染范围也就会越大。病毒的内部有一种触发机制，不满足触发条件时，病毒除了传染外不做什么破坏。一旦触发条件得到满足，病毒便开始表现，有的只是在屏幕上显示信息、图形或特殊标识，有的则执行破坏系统的操作，如格式化磁盘、删除文件、加密数据、封锁键盘、毁坏系统等。触发条件可能是预定时间或日期、特定数据出现、特定事件发生等。

（4）多态性

病毒试图在每一次感染时改变它的形态，使对它的检测变得更困难。一个多态病毒还是原来的病毒，但不能通过扫描特征字符串来发现。病毒代码的主要部分相同，但表达方式发生了变化，也就是同一程序由不同的字节序列表示。

（5）破坏性

病毒一旦被触发而发作就会造成系统或数据的损伤甚至毁灭。病毒都是可执行程序，而且又必然要运行，因此所有的病毒都会降低计算机系统的工作效率，占用系统资源，其侵占程度取决于病毒程序自身。病毒的破坏程度主要取决于病毒设计者的目的，如果病毒设计者的目的在于彻底破坏系统及其数据，那么这种病毒对于计算机系统进行攻击造成的后果是难以想像的，它可以毁掉系统的部分或全部数据并使之无法恢复。虽然不是所有的病毒都对系统产生极其恶劣的破坏作用，但有时几种本没有多大破坏作用的病毒交叉感染，也会导致系统崩溃等重大恶果。

14.2.2 计算机病毒的结构

计算机病毒主要由潜伏机制、传染机制和表现机制构成。在程序结构上由实现这3种机制的模块组成（见图 14-1）。

若某程序被定义为计算机病毒，只有传染机制是强制性的，潜伏机制和表现机制是非强制性的。

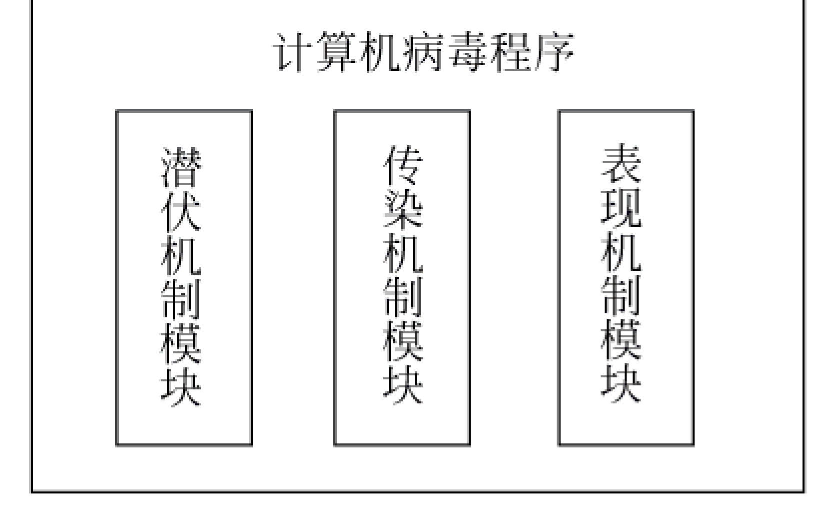


图 14-1　计算机病毒程序结构

1. 潜伏机制

潜伏机制的功能包括初始化、隐藏和捕捉。潜伏机制模块随着感染的宿主程序的执行进入内存，首先，初始化其运行环境，使病毒相对独立于宿主程序，为传染机制做好准备。然后，利用各种可能的隐藏方式，躲避各种检测，欺骗系统，将自己隐蔽起来。最后，不停地捕捉感染目标交给传染机制，不停地捕捉触发条件交给表现机制。

2 传染机制

传染机制的功能包括判断和感染。传染机制先是判断候选感染目标是否已被感染，感染与否通过感染标记来判断，感染标记是计算机系统可以识别的特定字符或字符串。一旦发现作为候选感染目标的宿主程序中没有感染标记，就对其进行感染，也就是将病毒代码和感染标记放入宿主程序之中。早期的有些病毒是重复感染型的，它不做感染检查，也没有感染标记，因此这种病毒可以再次感染自身。

3. 表现机制

表现机制的功能包括判断和表现。表现机制首先对触发条件进行判断，然后根据不同的条件决定什么时候表现、如何表现。表现内容多种多样，然而不管是炫耀、玩笑、恶作剧，还是故意破坏，或轻或重都具有破坏性。表现机制反映了病毒设计者的意图，是病毒间差异最大的部分。潜伏机制和传染机制是为表现机制服务的。

14.3　防治措施

恶意代码或计算机病毒(这里把两者基本等同起来)带来的危害已经严重地影响了人们的工作和生活，威胁着社会的秩序和安全。全球对防治病毒的关注和重视不断升温，病毒防治技术也随之迅速发展，与病毒制造技术展开了前所未有的竞赛。病毒制造技术与病毒防治技术是“矛”与“盾”的辩证发展关系，互为发展动力。

防治病毒，顾名思义，一是“防”，二是“治”。“防”是主动的，“治”是被动的。首先要积极地“防”，尽量避免病毒入侵，然而“防”是有时效性的，今天防住了，明天就有可能被突破。对于入侵的病毒当然要努力地“治”，以尽量减少和挽回病毒造成的损失，并且通过“治”的过程掌握病毒的机理，反过来又可以加强“防”了。因此，病毒防治应采取“以防为主、与治结合、互为补充”的策略，不可偏废任何一方面。

14.3.1　病毒防治的技术

如上所述，病毒防治技术分为“防”和“治”两部分。“防”毒技术包括预防技术和免疫技术；“治”毒技术包括检测技术和消除技术。

1. 病毒预防技术

病毒预防是指在病毒尚未入侵或刚刚入侵还未发作时，就进行拦截阻击或立即报警。要做到这一点，首先要清楚病毒的传播途径和寄生场所，然后对可能的传播途径严加防守，对可能的寄生场所实时监控，达到封锁病毒入口，杜绝病毒载体的目的。不管是传播途径的防守还是寄生场所的监控，都需要一定的检测技术手段来识别病毒。有关病毒识别的检测技术，将在病毒检测技术一节中详细介绍。

病毒的传播途径和寄生场所都是实施病毒预防措施的对象。

(1) 病毒的传播途径及其预防措施

① 不可移动的计算机硬件设备，包括 ROM 芯片、专用 ASIC 芯片和硬盘等。目前的

个人计算机主板上分离元器件和小芯片很少，主要靠几块大芯片，除 CPU 外其余的大芯片都是 ASIC 芯片。利用先进的集成电路工艺，在芯片内可制作大量的单元电路，集成各种复杂的电路。这种芯片带有加密功能，除了知道密码的设计者外，写在芯片中的指令代码没人能够知道。如果将隐藏有病毒代码的芯片安装在敌对方的计算机中，通过某种控制信号激活病毒，就可对敌手实施出乎意料的、措手不及的打击。这种新一代的电子战、信息战的手段已经不是幻想。在 1991 年的海湾战争中，美军对伊拉克部队的电脑防御系统实施病毒攻击，成功地使该系统一半以上的计算机染上病毒，遭受破坏。这种病毒程序具有很强的隐蔽性、传染性和破坏性；在没有收到指令时会静静地隐藏在专用芯片中，极不容易发现；一旦接到指令，便会发作，不断扩散和破坏。这种传播途径的病毒很难遇到，目前尚没有较好的发现手段对付。

具体预防措施包括：

- 对于新购置的计算机系统用检测病毒软件或其他病毒检测手段（包括人工检测方法）检查已知病毒和未知病毒，并经过实验，证实没有病毒感染和破坏迹象后再实际使用。
- 对于新购置的硬盘可以进行病毒检测，更保险起见也可以进行低级格式化。注意，对硬盘只做 DOS 的 Format 格式化不能除去主引导区中的病毒。

② 可移动的存储介质设备，包括软盘、磁带、光盘以及可移动式硬盘等。软盘曾是使用最广泛、携带最便利、移动最频繁的存储介质，因此，成了计算机病毒寄生的“温床”，大多数计算机都是从这类途径感染病毒的。

具体预防措施包括以下几项：

- 在保证硬盘无病毒的情况下，尽量用硬盘而不要用软盘启动计算机。启动前，要保证软盘驱动器中无任何软盘。注意，即使不是系统盘，染毒的数据盘也会将病毒带入系统。
- 尽量将程序文件和数据文件分开存放在不同的软盘中，将装有程序文件的软盘设置到写保护状态。目前还没有只用软件就可以避开写保护的方法。
- 建立封闭的使用环境，即做到专机、专人、专盘和专用。如果通过软盘等与外界交互，不管是自己的软盘在别人的机器上用过，还是别人的软盘在自己的机器上使用，都要进行病毒检测。
- 任何情况下，保留一张写保护的、无病毒的并带有各种基本系统命令的系统启动软盘。一旦系统出现故障，不管是因为染毒或是其他原因，就可用于恢复系统。

③ 计算机网络，包括局域网、城域网、广域网，特别是 Internet。各种网络应用（如 E-mail、FTP、Web 等）使得网络途径更为多样和便捷。计算机网络是病毒目前传播最快、最广的途径，由此造成的危害蔓延最快、数量最大。从 1988 年的 Morris 蠕虫开始，席卷全球的网络蠕虫事件一浪接一浪，愈演愈烈。

具体预防措施包括以下几项：

- 采取各种措施保证网络服务器上的系统、应用程序和用户数据没有染毒，如坚持用硬盘引导启动系统，经常对服务器进行病毒检查等。
- 将网络服务器的整个文件系统划分成多卷文件系统，各卷分别为系统、应用程序

和用户数据所独占，即划分为系统卷、应用程序卷和用户数据卷。这样各卷的损伤和恢复是相互独立的，十分有利于网络服务器的稳定运行和用户数据的安全保障。

- 除网络系统管理员外，系统卷和应用程序卷对其他用户设置的权限不要大于只读，以防止一般用户的写操作带进病毒。
- 系统管理员要对网络内的共享区域，如电子邮件系统、共享存储区和用户数据卷进行病毒扫描监控，发现异常及时处理，防止在网上扩散。
- 在应用程序卷中提供最新的病毒防治软件，为用户下载使用。
- 严格管理系统管理员的口令，为了防止泄露应定期或不定期地进行更换，以防非法入侵带来病毒感染。
- 由于不能保证网络，特别是 Internet 上的在线计算机百分之百地不受病毒感染，所以，一旦某台计算机出现染毒迹象，应立即隔离并进行排毒处理，防止它通过网络传染其他计算机。同时，密切观察网络及网络上的计算机状况，以确定是否已被病毒感染。如果网络已被染毒，应马上采取进一步的隔离和排毒措施，尽可能地阻止传播、减小传播范围。
- 网络是蠕虫传播的最重要途径，尤其通过电子邮件传播。为了预防和减少邮件蠕虫病毒的危害，可采取如下方法：
  - 设定邮件的路径在 C：以外，因为 C 分区是病毒攻击频率最高的地方，这样既可减轻对 C 分区的病毒攻击，万一情况下也可减少损失。
  - 收到新邮件后，尽量使用“另存为”选项为邮件做备份，分类存储，避免在同一根目录下放全部的邮件。既做到备份，又方便管理和查阅，一举两得。
  - 在“通讯簿”尽量不要设置太多的名单，如果要发送新邮件，可以进入邮件的储存目录，打开客户发来的邮件，利用“回复”功能来发送新邮件（删除原有内容即可）；如果客户较多，可建立一个文本文件存放所有客户的邮件地址，要发新邮件时，利用“粘贴”功能把客户邮件地址复制到“收件人”栏中去。这样能够有效地防止邮件蠕虫病毒通过“通讯簿”的进一步传播。
  - 遇到可执行文件（*.EXE、*.COM）或有宏功能文档（*.DOC 等）的附件，不要打开，先选择为“另存为”到磁盘上，用病毒防治软件先进行检查和杀毒后再使用。

④ 点对点通信系统，指两台计算机之间通过串行/并行接口，或者使用调制解调器经电话网进行数据交换。

具体预防措施为，通信之前对两台计算机进行病毒检测，确保没有病毒感染。

⑤ 无线通信网，作为未来网络的发展方向，无线通信网会越来越普及，同时也将会成为与计算机网络并驾齐驱的病毒传播途径。

具体预防措施可参照计算机网络的预防措施。

（2）病毒的寄生场所及其预防措施

① 引导扇区，即软盘的第一物理扇区或硬盘的第一逻辑扇区，是引导型病毒寄生的地方。

具体预防措施为，用 Bootsafe 等实用工具或 DEBUG 编程等方法对干净的引导扇区

进行备份。备份既可用于监控，又可用于系统恢复。监控是比较当前引导扇区的内容和干净的备份，如果发现不同，则很可能是感染了病毒。

② 计算机文件，包括可执行的程序文件、含有宏命令的数据文件，是文件型病毒寄生的地方。

具体预防措施包括以下几项：

- 检查.COM 和.EXE 可执行文件的内容、长度、属性等，判断是否感染了病毒。重点检查可执行文件的头部(前 20 个字节左右)，因为病毒主要改写文件的起始部分。病毒代码可能就在文件头部，即使在文件尾部或其他地方，文件头部中也必有一条跳转指令指向病毒代码。
- 对于新购置的计算机软件要进行病毒检测。
- 定期与不定期地进行文件的备份。备份既可通过比较发现病毒，又可用作灾难恢复。
- 为了预防宏病毒，将含有宏命令的模板文件，如常用的 Word 模板文件改为只读属性，可防止 Word 系统被感染，DOS 系统下的 autoexec.bat 和 config.sys 文件最好也都设为只读属性文件。将自动执行宏功能禁止掉，这样即使有宏病毒存在，但无法激活，能起到防止病毒发作的效果。

③ 内存空间，病毒在传染或执行时，必然要占用一定的内存空间，并驻留在内存中，等待时机再进行传染或攻击。

具体预防措施为，采用 PCTOOLS、DEBUG 等软件工具，检查内存的大小和内存中的数据来判断是否有病毒进入。

病毒驻留内存后，为了防止被系统覆盖，通常要修改内存控制块中的数据。如果检查出来的内存可用空间为 635KB，而真正配置的内存空间为 640KB，则说明有 5KB 内存空间被病毒侵占。

系统一些重要的数据和程序放在内存的固定位置，如 DOS 系统启动后，BIOS、变量、设备驱动程序等放在内存的 0:4000H～0:4FF0H 区域内，可以首先检查这些地方是否有异常。

④ 文件分配表(FAT)，病毒隐藏在磁盘上时，一般要对存放的位置做出“坏簇”标志反映在 FAT 表中。

具体预防措施为，检查 FAT 表有无意外坏簇来判断是否感染了病毒。

⑤ 中断向量，病毒程序一般采用中断的方式执行，即修改中断变量，使系统在适当的时候转向执行病毒程序，在病毒程序完成传染或破坏目的后，再转回执行原来的中断处理程序。

具体预防措施为，检查中断向量有无变化来确定是否感染了病毒。

2 病毒免疫技术

病毒具有传染性。一般情况下，病毒程序在传染完一个对象后，都要给被传染对象加上感染标记。传染条件的判断就是检测被攻击对象是否存在这种标记，若存在这种标记，则病毒程序不对该对象进行传染；若不存在这种标记，病毒程序就对该对象实施传染。

最初的病毒免疫技术就是利用病毒传染这一机理，给正常对象加上这种标记，使之具有免疫力，从而可以不受病毒的传染。因此，当感染标记用作免疫时，也叫做免疫标记。例如，使用这种技术可有效地防御香港病毒、1575 病毒等。

然而，有些病毒在传染时不判断是否存在感染标记，病毒只要找到一个可传染对象就进行一次传染。就像黑色星期五病毒那样，一个文件可能被该病毒反复传染多次，滚雪球一样越滚越大。其实，黑色星期五病毒的程序中具有判别感染标记的代码，由于程序设计错误，使判断失效，形成现在的情况，对文件会反复感染，感染标记形同虚设。

目前，常用的病毒免疫方法有两种：

(1) 针对某一种病毒进行的免疫方法

例如，对小球病毒，在 DOS 引导扇区的 1FCH 处填上 1357H，小球病毒一检查到这个标记就不再对它进行传染了。又如，对于 1575 文件型病毒，免疫标记是文件尾的内容为 0CH 和 0AH 的两个字节，1575 病毒若发现文件尾含有这两个字节，则不进行传染。

这种方法对防止某一种特定病毒的传染行之有效，但也存在一些缺点，主要有以下几点：

① 对于不设有感染标记的病毒不能达到免疫的目的，这种病毒会无条件传染，而不论被传染对象是否已经被感染过或者是否具有感染标记。

② 当某种病毒的变种不再使用其感染标记时，或出现新病毒时，现有免疫标记就发挥不了作用。

③ 一些病毒的感染标记不容易仿制，如非要加上这种标记不可，则对原来的文件要做大的改动。例如，对大麻病毒就不容易做免疫标记。

④ 由于病毒的种类较多，又由于技术上的原因，不可能对一个对象加上各种病毒的免疫标记，这就使得该对象不能对所有的病毒具有免疫作用。

⑤ 这种方法能阻止传染，却不能阻止病毒的破坏行为，仍然放任病毒驻留在内存中。

目前使用这种免疫方法的商品化防治病毒软件已不多见了。

(2) 基于自我完整性检查的免疫方法

目前，这种方法只能用于文件而不能用于引导扇区。这种方法的工作原理是，为可执行程序增加一个免疫外壳，同时在免疫外壳中记录有关用于恢复自身的信息。免疫外壳占 1KB 至 3KB。执行具有这种免疫功能的程序时，免疫外壳首先得到运行，检查自身的程序大小、校验和、生成日期和时间等情况，没有发现异常后，再转去执行受保护的程序。若不论什么原因使这些程序本身的特性受到改变或破坏，免疫外壳都可以检查出来，并发出告警，由用户选择应采取的措施，包括自毁、重新引导启动计算机、自我恢复后继续运行。这种免疫方法是一种通用的自我完整性检验方法，它不只是针对病毒，由于其他原因造成的文件变化同样能够检查出来，在大多数情况下免疫外壳程序都能使文件自身得到复原。

但这种免疫方法也有其缺点和不足，归纳如下：

① 每个受到保护的文件都要增加 1KB 至 3KB，需要额外的存储空间。

② 现在使用的一些校验码算法不能满足检测病毒的需要，被某些种类的病毒感染的文件不能被检查出来。

③ 无法对付覆盖式的文件型病毒。

④ 有些类型的文件不能使用外加免疫外壳的防护方法，这样会使那些文件不能正常执行。

⑤ 当某些尚不能被病毒检测软件检查出来的病毒感染了一个文件，而该文件又被免疫外壳包在里面时，这个病毒就像穿了“保护盔甲”，使查毒软件查不到它，而它却能在得到运行机会时跑出来继续传染扩散。

尽管尚不存在完美和通用的病毒免疫方法，但它在病毒防御措施中仍占一席之地。

3. 病毒检测技术

病毒检测就是采用各种检测方法将病毒识别出来。识别病毒包括对已知病毒的识别和对未知病毒的识别。目前，对已知病毒的识别主要采用特征判定技术，即静态判定技术，对未知病毒的识别除了特征判定技术外，还有行为判定技术，即动态判定技术。

(1) 特征判定技术

特征判定技术是根据病毒程序的特征，如感染标记、特征程序段内容、文件长度变化、文件校验和变化等，对病毒进行分类处理，而后在程序运行中凡有类似的特征点出现，则认定是病毒。

特征判定技术主要有以下几种方法：

① 比较法。比较法的工作原理是，将可能的感染对象(引导扇区或计算机文件)与其原始备份进行比较，如果发现不一致则说明有染毒的可能性。这种比较法不需要专门的查毒程序，用常规的具有比较功能的(如 PCTOOLS 等)工具软件就可以进行。比较法不仅能够发现已知病毒，还能够发现未知病毒。保留好干净的原始备份对于比较法非常重要；否则比较就失去了意义，比较法也就不起作用了。

比较法的优点是简单易行，不需要专用查毒软件，但缺点是无法确认发现的异常是否真是病毒，即使是病毒也不能识别病毒的种类和名称。

② 扫描法。也叫搜索法，其工作原理是，用每一种病毒代码中含有的特定字符或字符串对被检测的对象进行扫描，如果在被检测对象内部发现某一种特定字符或字符串，则表明发现了该字符或字符串代表的病毒。前面介绍传染机制时提到的感染标记就是一种识别病毒的特定字符。实现这种扫描的软件叫做特征扫描器。根据扫描法的工作原理，特征扫描器由病毒特征码库和扫描引擎两部分组成。病毒特征码库包含了经过特别选定的各种病毒的反映其特征的字符或字符串。扫描引擎利用病毒特征码库对检测对象进行匹配性扫描，一旦有匹配便发出告警。显然，病毒特征码库中的病毒特征码越多，扫描引擎能识别的病毒也就越多。病毒特征码的选择非常重要，一定要具有代表性，也就是说，在不同环境下，使用所选的特征码都能够正确地检查出它所代表的病毒。如果病毒特征码选择得不准确，就会带来误报(发现的不是病毒)或漏报(真正病毒没有发现)。

特征扫描器的优点是能够准确地查出病毒并确定病毒的种类和名称，为消除病毒提供了确切的信息，但其缺点是只能查出载入病毒特征码库中的已知病毒。特征扫描器是目前最流行的病毒防治软件。随着新病毒的不断发现，病毒特征码库必须不断丰富和更新。现在绝大多数的商业病毒防治软件商，提供每周甚至每天一次的病毒特征码库在线

更新。

③ 校验和法。校验和法的工作原理是，计算正常文件内容的校验和，将该校验和写入文件中或写入别的文件中保存。在文件使用过程中，定期地或每次使用文件前，检查文件当前内容算出的校验和与原来保存的校验和是否一致，如果不一致便发出染毒报警。

这种方法既能发现已知病毒，也能发现未知病毒，但是，它不能识别病毒种类，不能报出病毒名称。由于病毒感染并非文件内容改变的唯一的排他性原因，文件内容的改变有可能是正常程序引起的，如软件版本更新、变更口令以及修改运行参数等，所以，校验和法常常有虚假报警，而且此法也会影响文件的运行速度。另外，校验和法对某些隐蔽性极好的病毒无效。这种病毒进驻内存后，会自动剥去染毒程序中的病毒代码，使校验和法受骗，对一个有毒文件算出正常校验和。因此，校验和法的优点是方法简单、能发现未知病毒、被查文件的细微变化也能发现；其缺点是必须预先记录正常态的校验和、会有虚假报警、不能识别病毒名称、不能对付某些隐蔽性极好的病毒。

④ 分析法。分析法是针对未知的新病毒采用的技术。分析法的工作过程如下：

- 确认被检查的磁盘引导扇区或计算机文件中是否含有病毒。
- 确认病毒的类型和种类，判断它是否是一种新病毒。
- 分析病毒程序的大致结构，提取识别用的特征字符或字符串，用于添加到病毒特征码库中。
- 分析病毒程序的详细结构，为制定相应的反病毒措施提供方案。

分析法对使用者的要求很高，不但要具有较全面的计算机及操作系统的知识，还要具备专业的病毒方面的知识。一般使用分析法的人不是普通用户，而是反病毒技术人员。使用分析法需要 DEBUG、Proview 等分析工具程序和专用的试验用计算机。即使是很熟练的反病毒技术人员，使用功能完善的分析软件，也不能保证在短时间内将病毒程序完全分析清楚，病毒有可能在分析阶段继续传染甚至发作，毁坏整个软盘或硬盘内的数据，因此，分析工作一定要在专用的试验用机上进行。很多病毒采用了自加密和抗跟踪等技术，使得分析病毒的工作经常是冗长和枯燥的，特别是某些文件型病毒的程序代码长达 10KB 以上，并与系统牵扯的层次很深，使详细的剖析工作变得十分复杂。

（2）行为判定技术

识别病毒是以病毒的机理为基础，不仅识别现有病毒，而且以现有病毒的机理设计出对一类病毒（包括基于已知病毒机理的未来新病毒或变种病毒）的识别方法，其关键是对病毒行为的判断。行为判定技术就是要解决如何有效辨别病毒行为与正常程序行为，其难点在于如何快速、准确、有效地判断病毒行为。如果处理不当，就会带来虚假报警，就像“狼来了”的寓言一样，频频虚假报警的后果是报警不再引起用户的警惕。另外，防毒对于不按现有病毒机理设计的新病毒也可能无能为力，如在 DIR2 病毒出现之前推出的防病毒软件，几乎没有一个能控制该病毒，原因就在于该病毒的机理已经超出当时的防病毒软件所考虑的范围。如今，该病毒的机理已被人们认识，所以新推出的防病毒软件和防病毒卡，几乎没有一个不能控制该病毒及其变种病毒的。

行为监测法是常用的行为判定技术，其工作原理是利用病毒的特有行为特性进行监测，一旦发现病毒行为则立即报警。经过对病毒多年的观察和研究，人们发现病毒的一些

行为是病毒的共同行为，而且比较特殊。在正常程序中，这些行为比较罕见。监测病毒的行为特征列举如下：

① 占用 INT 13H。引导型病毒攻击引导扇区后，一般都会占用 INT 13H 功能，在其中放置病毒所需的代码，因为其他系统功能还未设置好，无法利用。

② 修改 DOS 系统数据区的内存总量。病毒常驻内存后，为了防止 DOS 系统将其覆盖，必须修改内存总量。

③ 向.COM 和.EXE 可执行文件做写入动作。写.COM 和.EXE 文件是文件型病毒的主要感染途径之一。

④ 病毒程序与宿主程序的切换。染毒程序运行时，先运行病毒，而后执行宿主程序。在两者切换时，有许多特征行为。

行为监测法的长处在于可以相当准确地预报未知的多数病毒，但也有其短处，即可能虚假报警和不能识别病毒名称，而且实现起来有一定难度。

不管采用哪种判定技术，一旦病毒被识别出来，就可以采取相应措施，阻止病毒的下列行为：进入系统内存、对磁盘操作尤其是写操作、进行网络通信与外界交换信息。一方面防止外界病毒向机内传染，另一方面抑制机内病毒向外传播。

4. 病毒消除技术

病毒消除的目的是清除受害系统中的病毒，恢复系统的原始无毒状态。具体来讲，就是针对系统中的病毒寄生场所或感染对象进行一一杀毒。对于不同的病毒类型及其感染对象，采取不同的杀毒措施。

(1) 消除引导型病毒

引导型病毒的物理载体是磁盘，主要包括系统软盘、数据软盘和硬盘。

① 修复染毒的系统软盘。找一台同样操作系统的未染毒的计算机，把染毒的系统软盘插入软盘驱动器中，从硬盘执行可以对软盘重新写入系统的命令，如 DOS 系统情况下的 SYS A:命令。这样软盘上的系统文件就会被重新安装，并且覆盖引导扇区中染毒的内容，从而恢复成为干净的系统软盘。

② 修复染毒的数据软盘。把染毒的数据软盘插入一台未染毒的计算机中，把所有文件从软盘复制到硬盘的一个临时目录中，用系统磁盘格式化命令，如 DOS 系统情况下的 FORMAT A:/U 命令，无条件重新格式化软盘，这样软盘的引导扇区会被重写，从而清除其中的病毒。然后把所有文件备份复制回到软盘。

③ 修复染毒的硬盘。硬盘中操作系统的引导扇区包括第一物理扇区和第一逻辑扇区。硬盘第一物理扇区存放的数据是主引导记录(MBR)，MBR 包含表明硬件类型和分区信息的数据。硬盘第一逻辑扇区存放的数据是分区引导记录。主引导记录和分区引导记录都有感染病毒的可能性。重新格式化硬盘可以清除分区引导记录中的病毒，却不能清除主引导记录中的病毒。修复染毒的主引导记录的有效途径是使用 FDISK 这种低级格式化工具，输入 FDISK/MBR，便会重新写入主引导记录，覆盖掉其中的病毒。

以上均是采用人工方法清除引导型病毒。人工方法要求操作者对系统十分熟悉，且操作复杂，容易出错，有一定的危险性，一旦操作不慎就会导致意想不到的后果。这种方

法常用于消除自动方法无法消除的新病毒。

另外一种是自动方法，针对某一种或多种病毒采用专门的病毒防治软件自动检测和消除病毒。这种方法不会破坏系统数据，操作简单，运行速度快，是一种较为理想且目前较为通用的病毒防治方法。

大多数病毒防治软件能够检测和清除已知的引导型病毒。通过监测磁盘的引导扇区，包括硬盘的主引导记录(MBR)，可以自动检测出病毒，并准确识别病毒，包括病毒的类型和名称；然后自动修复被感染的引导扇区。

(2) 消除文件型病毒

文件型病毒的载体是计算机文件，包括可执行的程序文件和含有宏命令的数据文件。

修复染毒的可执行文件最有效的方法是用干净的备份代替它。如果没有备份，就使用病毒防治软件进行检测、杀毒并修复。对于被非覆盖型病毒感染的文件，病毒防治软件有可能将其修复，但对于覆盖型病毒就无能为力了。

非覆盖型病毒感染可执行文件时，只是将自身附加到感染对象的头部或尾部或其他空白地方，并没有破坏文件的有效内容，而且必须存放有关宿主程序的特定信息，以便自己执行完后把控制权交还给原来的程序。因此，病毒防治软件可以根据这一特定信息定位病毒，然后“顺藤摸瓜”，将病毒从文件中“切掉”。

(3) 消除宏病毒

宏病毒是一种文件型病毒，其载体是含有宏命令的数据文件——文档或模板。

手工清除方法为：

① 在空文档的情况下，打开宏菜单，在通用模板中删除被认为是病毒的宏。

② 打开带有病毒宏的文档或模板，然后打开宏菜单，在通用模板和定制模板中删除认为是病毒的宏。

③ 保存清洁的文档或模板。

自动清除方法有：

① 用 WordBasic 语言以 Word 模板方式编制杀毒工具，在 Word 环境中杀毒。这种方法杀毒准确，兼容性好。

Word-VRV 就是采用这种方法的典型杀毒工具。Word-VRV 由 WORDVRV. DOT(用于中文版 Word)、EWORD-VRV. DOT(用于英文版 Word)和 README. EXE 3 个文件组成。Word-VRV 是个可自升级的 Word 杀毒器，可自动检测并清除 Word 模板中的病毒。Word-VRV 允许用户通过编辑 WORDVRV. DAT 文件，自我扩充新的宏病毒特征，来杀除新的宏病毒。

② 根据 WordBFF 格式，在 Word 环境外解剖病毒文档或模板，去掉病毒宏。由于各个版本的 WordBFF 格式都不完全兼容，每次 Word 升级它也必须跟着升级，兼容性不太好。

(4) 消除蠕虫病毒

蠕虫病毒是蠕虫和病毒的混合体，即具有病毒的传染机制，又具有蠕虫的自我复制和网络传播的机制。消除蠕虫病毒从本机杀毒和网络封锁两个方面同时进行，才是万全之策。清除了本机病毒，就消灭了病毒源；截获了网络蠕虫，就切断了病毒的网络传

播途径。

① 清除本机病毒。根据病毒的感染对象，采取上述相应的人工或自动杀毒方法。

② 截获网络蠕虫。在网络入出口处，特别是电子邮件的收发，采取人工的或自动的方法截获蠕虫。人工的方法是，网络管理员和电子邮件用户，根据蠕虫病毒的活动规律，主动识别收发信息中的蠕虫病毒，主要是病毒防治软件不能识别的可疑的或新的蠕虫病毒。自动的方法是，在网络入出口处，安装病毒防治软件，监控入出信息，一旦发现病毒，立即截获并消除。

14.3.2　病毒防治的部署

有效的病毒防治部署是采用基于网络的多层次的病毒防御体系。该体系在整个网络系统的各组成环节处，包括客户端、服务器、Internet 网关和防火墙，设置防线，形成多道防线。即使病毒突破了一道防线，还有第二、三道防线拦截，因此，能够有效地遏制病毒在网络上的扩散。

（1）客户端防线

客户端主要是指用户桌面系统和工作站，它们是主要的病毒感染源。因此，有必要在客户端实施面向桌面系统和工作站的病毒防治措施，增强客户端系统的抗病毒能力。对于有相当规模的企业网络系统，工作站的病毒防治系统应该具有集中管理、统一策略、同时更新和自动运行的特点。

（2）服务器防线

服务器是基于网络的各种服务的提供者，被大量的在线用户访问，一旦染毒，其后果将不堪设想。因此，非常有必要在服务器实施最严格的病毒防治措施，确保服务器系统的万无一失。尤其，对于电子邮件服务器，如 Microsoft Exchange 和 Lotus Notes/Domino 服务器，要特别重点保护，因为电子邮件是目前传播最快、范围最广、危害最大的蠕虫病毒的最主要的传播途径。

（3）Internet 网关防线

在 Internet 网关处装备病毒扫描器可有效地对付以 Internet 应用为载体的病毒，包括通过电子邮件传播的病毒。

（4）防火墙防线

在防火墙设置病毒扫描器，可以扫描到经过防火墙的所有网络数据帧，因此，有条件全面地检测和阻止内外网络交接处的病毒。

14.3.3　病毒防治的管理

病毒防治不仅是技术问题，更是社会问题、管理问题和教育问题。作为社会问题，涉及国家法律和行政法规；作为管理问题，涉及管理制度、行为规章和操作规程；作为教育问题，涉及宣传和培训。因此，要做到以下几点：

- 建立和健全相应的国家法律和法规；
- 建立和健全相应的管理制度和规章；
- 加强和普及相应的知识宣传和培训。

14.3.4　病毒防治软件

1. 病毒防治软件的类型

病毒防治软件按其查毒杀毒机制可分为以下 3 种类型：

（1）病毒扫描型

病毒扫描型软件采用特征扫描法，根据病毒特征扫描可能的感染对象来发现病毒。这类软件具有检测速度快、误报率低和准确度高的优点，正因为能准确识别已知病毒，所以对被已知病毒感染的程序和数据一般都能恢复。但是，要一直保证病毒防治的有效性，病毒特征码库和扫描引擎必须经常升级，以便跟上病毒技术和反病毒技术的发展。病毒防治软件中以病毒扫描型为主，是最为流行的产品。

（2）完整性检查型

完整性检查型软件采用比较法和校验和法，监视观察对象（包括引导扇区和计算机文件等）的属性（包括大小、时间、日期和校验和等）和内容是否发生改变，如果检测出变化，则观察对象极有可能已遭病毒感染。遗憾的是这类软件只能在发生病毒感染之后，才能发现病毒，而且“误诊”率相对较高，这是因为正常的程序升级和设置改变等原因都可以导致“误诊”。另外，尽管这类软件不能报出病毒的类型和名称，但能够发现多态病毒和新的未知病毒，所以反病毒的能力相当强。

（3）行为封锁型

行为封锁型软件采用驻留内存在后台工作的方式，监视可能因病毒引起的异常行为，如果发现异常行为，便及时警告用户，由用户决定该行为是否继续。这类软件试图阻止任何病毒的异常行为，因此可以防止新的未知病毒的传播和破坏。当然，有的“可疑行为”是正常的，所以出现“误诊”总是难免的。

这种监视技术的进一步发展和完善就是智能式探测器。在智能式探测器中，设计有病毒行为知识库、应用人工智能技术、有效判别正常程序行为和病毒程序行为。误报率的高低取决于行为知识库选取的合理性。目前，有些病毒防治卡采用了这种技术，设计有病毒特征码库（静态）、病毒行为知识库（动态）、受保护对象行为知识库（动态）等多个知识库及相应的可变推理机，通过调整推理机，能够对付新类型病毒，减少误报和漏报。这是未来病毒防治技术的一个发展方向。

2 病毒防治软件的选购

选购病毒防治软件时，需要注意的指标包括检测速度、识别率、清除效果、可管理性、操作界面友好性、升级难易度、技术支持水平等诸多方面。

（1）检测速度

对于采用特征扫描法检测病毒的，一般选择每 30 秒能够扫描 1000 个文件以上的病毒防治软件。

（2）识别率

识别率越高，误报率和漏报率也就越低。可通过使用一定数量的病毒样本进行测试

来鉴别识别率的高低，测试环境应达到正规的病毒样本测试数量在 10 000 种以上，每种病毒的变种数量在 200 种以上。

（3）清除效果

可靠、有效地清除病毒，并保证数据的完整性，是一件非常必要且复杂的工作。

① 对于被感染的引导扇区，虽不一定要求恢复被破坏软盘的引导功能，但要求能够恢复被破坏硬盘的引导过程；否则不能算病毒清除成功。

② 对于被感染的可执行文件，不必要求清除后的文件与正常文件一模一样，只要可以正常、正确地运行即可。

③ 对于含有宏病毒的文档文件，要求能够清除其中的宏病毒，保留正常的宏语句。

④ 对于病毒的变种，优秀的病毒防治软件不仅能够正确识别已有的病毒变种，而且也能够修复感染对象，使其正常工作。测试病毒防治软件对病毒变种的适应能力，是对产品质量和技术水平的最好评估。

3. 病毒防治软件产品

下面列出国内外主要的病毒防治产品及其查询网址。

（1）国外病毒防治产品

① VirusScan，网址 http://www.mcafeeb2b.com/。

② NAV，网址 http://www.symantec.com/。

③ Pandaguard，网址 http://www.pandaguard.com/。

（2）国内病毒防治产品

① KILL，网址 http://www.kill.com.cn/。

② KV，网址 http://www.jiangmin.com/。

③ RAV，网址 http://www.rising.com.cn/。

④ VRV，网址 http://www.vrv.com.cn/。

14.4 本章小结

恶意代码是指黑客编写的扰乱社会和他人甚至起着破坏作用的计算机程序，计算机病毒是恶意代码中最常见的一种。为了保障计算机系统和网络的正常运行，有必要懂得恶意代码与计算机病毒的基本概念、工作原理和防止措施。

恶意代码按照是否需要宿主和是否能够自我复制分为 4 大类：

（1）不感染的依附性恶意代码，包括特洛伊木马、逻辑炸弹、后门或陷门等。

（2）不感染的独立性恶意代码，包括点滴器、繁殖器、恶作剧等。

（3）可感染的依附性恶意代码，主要是病毒。

（4）可感染的独立性恶意代码，包括蠕虫、细菌等。

计算机病毒的基本特征有传染性、隐蔽性、潜伏性、多态性和破坏性。计算机病毒主要由潜伏机制、传染机制和表现机制构成。

恶意代码或计算机病毒的防治应采取“以防为主、与治结合、互为补充”的策略，不可偏废任何一方面。病毒防治技术包括预防技术、免疫技术、检测技术和消除技术。有效的病毒防治部署采用基于网络的多层次的病毒防御体系。

病毒防治不仅是技术问题，更是社会问题、管理问题和教育问题，应建立和健全相应的国家法律和法规，建立和健全相应的管理制度和规章，加强和普及相应的知识宣传和培训。

病毒防治软件按其查毒杀毒机制分为病毒扫描型、完整性检查型和行为封锁型。选购病毒防治软件时，需要注意的指标包括检测速度、识别率、清除效果、可管理性、操作界面友好性、升级难易度、技术支持水平等诸多方面。

习　题

1. 画出下面恶意代码类别与实例的对应关系。

类别	实例
A. 不感染、依附性	a. 后门(backdoor)
B. 不感染、独立性	b. 点滴器(dropper)
C. 可感染、依附性	c. 繁殖器(generator)
D. 可感染、独立性	d. 细菌(germ)
	e. 恶作剧(hoax)
	f. 逻辑炸弹(logic bomb)
	g. 陷门(trapdoor)
	h. 特洛伊木马(Trojan horse)
	i. 病毒(virus)
	j. 蠕虫(worm)

2. 计算机病毒有哪些基本特征？

3. 计算机病毒主要由(　)机制、(　)机制和(　)机制构成。

4. 计算机病毒按连接方式分为(　)、(　)、(　)和(　)，按破坏性质分为(　)和(　)，按感染方式分为(　)、(　)和(　)。

A. 良性病毒　　B. 源码型病毒　　C. 恶性病毒
D. 嵌入型病毒　　E. 引导型病毒　　F. 外壳型病毒
G. 文件型病毒　　H. 混合型病毒　　I. 操作系统型病毒

5. 宏病毒属于哪种类型的病毒？

6. 病毒防治技术分为“防”和“治”两部分。“防”毒技术包括(　)技术和(　)技术；“治”毒技术包括(　)技术和(　)技术。

7. 计算机病毒特征判定技术有(　)法、(　)法、(　)法和(　)法。

8. 基于网络的多层次的病毒防御体系中设置的多道防线包括(　)防线、(　)防线、(　)防线和(　)防线。

9. 病毒防治不仅是技术问题,更是(　)问题、(　)问题和(　)问题。

10. 病毒防治软件的类型分为(　)型、(　)型和(　)型。

第15章 系统平台安全

本章要点：

- 系统平台的概念、种类及安全风险；
- 系统平台通用加固指南及工具；
- Windows Server 2000 及 UNIX 系统安全设置和管理。

15.1 系统平台概述

15.1.1 系统平台的概念

系统平台是指网络操作系统(network operating system, NOS)平台，即使网络上各计算机能方便而有效地共享网络资源，为网络用户提供所需的各种服务软件和有关规程的集合。因此，网络操作系统可使一台计算机上的应用去访问接在同一网上的另一台计算机上的资源。

网络操作系统除了应具有通常操作系统应具有的处理机管理、存储器管理、设备管理和文件管理外，还应具有以下两大功能：高效、可靠的网络通信能力；多种网络服务功能，如远程作业录入与处理的服务功能、文件传输服务功能和远程打印服务功能。

网络操作系统有两个基本的要求：允许在局域网上的资源共享；要使现有的PC操作系统仍能继续运行，且不需做任何改变。为了满足这两个基本要求，有两个主要组成，最主要的组成是控制服务器的操作、管理存储在服务器上的文件。不同于PC操作系统的运行环境，在网上有多个用户在争用网上共享的资源，不同用户有不同的作业，因此网络操作系统需要支持多用户和多任务。第二个组成是运行在客户系统的软件，使客户能访问网络及网上资源，而这些资源和服务由网上服务器提供。

目前，较流行的网络操作系统有 Windows 9x 系列、Windows NT/2000/XP/2003/Vista 系列、UNIX 系列、Linux 系列及 NetWare 系列。

15.1.2 系统平台的种类

网络操作系统的主要功能是实现资源共享。根据共享资源的方式不同，网络操作系统划分为两大类型。如果网络操作系统软件相等地分布在网络上的所有结点，这种机制下的网络操作系统称之为对等式网络操作系统；如果网络操作系统的主要部分驻留在中心结点，则称为集中式网络操作系统。集中式网络操作系统下的中心结点称为服务器，使用由中心结点所管理资源的应用称为客户。因此，集中式网络操作系统下的运行机制就

是人们平常所谓的“客户端/服务器”方式。因为客户软件运行在工作站上,所以人们有时将工作站称为客户。其实只有使用服务的应用才能称为客户,向应用提供服务的应用或系统软件才能称为服务器。

对等式网络操作系统有多种,如 Novell 公司的 Personal NetWare,Invisible Software 公司的 Invisible LAN3.44,Microsoft 公司的 Windows for Workgroup 3.11、Windows 9x 等。用户期待对等式网络比客户端/服务器更容易操作,安装尽量简单,管理更加方便,具有内建的生产工具,并具有一定的安全级别,以防止敏感性数据受损害。

集中式网络操作系统也有多种,如 Novell 公司的 NetWare 3.x、4.x、5.x、6.x,Microsoft Windows NT/2000/2003,IBM OS/2 LAN Server Advanced 3.0 和 Banyan Vines 等都属于集中式网络操作系统。这种以客户端/服务器方式操作的网络操作系统,由于顺应 20 世纪 90 年代的计算模式,发展非常迅速。网络操作系统的功能比以前传统上只提供文件和打印共享的系统有了很大提高。例如 Novell 公司的 4.x 不再将网络看成一组无联系的服务器和服务,而是将其看作单个实体,同时还增加了完全符合 X.500 原理的目录服务等重要功能。

1. NetWare 系列

NetWare 是运行在 Intel 处理器平台上的网络操作系统,经过近 20 年开发,NetWare 经历了 NetWare 2.x,NetWare 3.x,NetWare 4.x,NetWare 5.x 及 NetWare 6.x 一系列阶段。作为典型的集中式网络操作系统,NetWare 由服务器及桌面客户机组成。

2. 微软 Windows 系列

Windows 系列网络操作系统既有点对点的对等网络操作系统,又有集中式服务器操作系统。Windows 9x/Me,Windows NT/2000 Workstation 及 Windows XP Professional/Home 代表了当今流行的点对点的对等桌面操作系统,而 Windows NT/2000/2003 Server 则代表了服务器操作系统。

3. UNIX 操作系统

严格来讲,UNIX 不是网络操作系统,但由于它能支持通信功能,并提供一些大型服务器操作系统的功能,因此也可把它作为 NOS。UNIX 的一个很大特点是灵活性,这使硬件制造商和软件开发者普遍采用 UNIX。但同时带来的问题是可移植性差,灵活性和可移植性是一对矛盾。为了解决兼容性,各个主要计算机厂商成立了一个协调组,致力于形成一个统一的 UNIX 系统版本,这些厂商包括 IBM、HP、Novell 以及 SCO,组成了一个名为 COSE (Common Open Software Environment,公用开放软件环境)的组织,从事这项工作。

4. Linux 操作系统

Linux 操作系统是 UNIX 操作系统在微机上的实现,它是由芬兰赫尔辛基大学的 Linus Torvalds 于 1991 年开始开发的,并在网上免费发行。Linux 是一个完全多任务、多用户的操作系统,允许多用户同时登录到一台机器上同时运行多道程序。Linux 在源代码级几乎与一些 UNIX 标准兼容,其中包括 IEEE POSIX.1、AT&T 系统 V 和 BSD。在

它的开发过程中一直以源代码的可移植性为原则。

15.1.3　系统平台的安全风险

风险是威胁和漏洞的组合，如果没有漏洞，也就没有风险。每个平台无论是硬件或软件，都存在着漏洞。作为网络安全的基础，网络操作系统也不例外。从某种意义上讲，系统平台的风险大小取决于网络操作系统漏洞的多少及严重程度。尽管众多的安全服务提供商及操作系统厂商不断花费大量人力财力来发现系统漏洞、修补漏洞，但不幸的是，漏洞并不因此而消除。据国际权威组织 SANS 及 FBI 公布的 2006 年安全漏洞表明，在排名前 20 名的 Internet 最严重的安全漏洞中，仍有 1/3 是网络操作系统的漏洞。

1. Windows 系列漏洞

（1）微软 IE 浏览器

微软的 IE 浏览器是安装 Windows 系列操作系统的默认安装。在未安装漏洞补丁程序或老版本的 IE 浏览器中存在多个安全漏洞，这些安全漏洞会导致内存内容被恶意篡改、欺骗及执行任意脚本文件。浏览器漏洞所导致的最致命问题是：在用户访问一个恶意网页或阅读电子邮件时，在用户不知情的情况下，远程执行一段漏洞代码，而这些利用 IE 漏洞的代码是因特网上公开的。此外，通过 IE 浏览器可能导致利用其他 Windows 核心组件（例如 HTML）帮助引擎及图形渲染引擎的安全漏洞来执行恶意代码。微软及其他第三方软件提供商所提供 ActiveX 控件中的安全漏洞也是通过 IE 浏览器安装的。

上述漏洞已被广泛用来安装间谍软件、广告软件及其他恶意程序于用户系统上，一些仿冒攻击也是通过欺骗漏洞产生的。

（2）Windows 系统库

Windows 系统库是若干程序模块组成，系统库中包含许多供其他模块调用的函数及数据，如 Windows 应用程序。通常，Windows 应用程序通过大量调用库函数以实现其功能，库函数往往被封装成动态链接库（DLL）的文件格式，并具有扩展名 DLL 或 OCX。动态链接库为系统提供了一种模块化应用程序的方法，使其功能易于复用，易于更新。当几个应用程序同时使用同一功能函数时，动态链接库也有助于减少内存使用开销。许多 Windows 的任务使用动态链接库，例如，HTML 语法检查，影像格式解码和协议解码等。由于本地及远程的应用程序都要使用动态链接库，因此，动态链接库中的一个漏洞将影响所有使用该库的系统应用程序及其他使用该动态库的第三方软件提供商所提供的软件。攻击者可以通过多种途径利用动态链接库的漏洞发动对系统的攻击，例如，通过 IE 浏览器、Office 办公软件及图像查看软件来利用图像处理动态链接库的漏洞。在许多情况下，远程攻击者只需要诱骗用户访问他们精心设计的网站，查看图像、点击图标或光标文件，攻击者即可以用户的权限执行任意代码。

（3）微软 Office 办公软件

微软 Office 办公软件是目前广为流行的收发电子邮件及日常办公套件。该套件包括 Outlook，Word，PowerPoint，Excel，Visio，FrontPage 及 Access。利用该套件中存在的

漏洞,攻击者可以通过以下途径发起攻击:

- 攻击者发送带有恶意 Office 文档的邮件,其中的病毒可以利用这种恶意 Office 文档进行系统间的相互传播;
- 攻击者将恶意 Office 文档放在 Web 服务器或共享文件夹中,而诱使用户浏览网页或共享文件夹。由于 IE 浏览器将自动打开 Office 文档,因此,当用户浏览了放有恶意 Office 文档的网页或文件夹后,攻击者即可利用该漏洞对系统发起攻击;
- 攻击者通过配置新闻服务器或劫持了 RSS 频道向邮件客户发送恶意文件。

(4) Windows 操作系统的服务程序

Windows 家族的操作系统提供各种服务、网络连接的方法和技术。所有的服务都是在统一的服务控制管理程序(SCM)的控制下,以服务控制程序(SCP)方式实现,服务控制管理程序的运行程序是 Services.exe。攻击者常常利用操作系统中服务控制程序的漏洞对操作系统发起攻击。负责向客户组件提供远程接口的几个系统核心组件使用了远程过程调用(RPC),这些核心组件通过使用 CIFS 协议经由命名的管道端点访问暴露出其安全缺陷,即已知的某些 TCP/UDP 通道及一些临时建立的 TCP/UDP 通道。历史上,系统服务中存在许多可以被匿名用户利用的漏洞,当攻击者利用服务中存在的漏洞攻击用户系统后,他们具有与系统服务一样的控制系统的权限。

在旧版本操作系统中,尤其是 Windows NT 和 Windows 2000 中,系统的默认配置是允许这些系统服务。

(5) Windows 系统配置缺陷

① 用户口令设置缺陷。

近年来,由于口令设置缺陷导致蠕虫病毒、蝇蛆(Bots)及其他恶意软件的大量繁殖及扩散。实行口令强度检查是一个 IT 管理员所面临的最古老的问题,但如今,仍然是给企业造成损失的主要原因。口令配置的缺陷存在于微软的本地口令系统及活动目录中,两者中的任意缺陷都能够被内部威胁及恶意软件所利用。此外,随着跨平台集中身份鉴别需求的不断增加,Windows 系统凭据的泄露将会导致其他平台系统凭据的泄露(例如 UNIX/RACF/ACF2/Top Secret)。

② 服务账号口令。

在 Windows 系统中,非系统的服务账号需要口令。但很不幸的是,这些口令通常使用了短的且可打印的字符串,最糟糕的是:它们常用于多台主机上,服务账号具有很高的对系统的访问权限,且账号的口令很少变更。

③ 匿名登录。

匿名是 Windows 域环境下长期存在的问题。在早期的 Windows NT 域结构中,空会话允许匿名用户枚举域中的主机系统、共享文件及用户账号。Windows 2000 系统在匿名访问上引入了两级控制方法,然而,该控制方法在系统的默认配置中是禁用的。在 Windows 2003 的早期版本中,微软为 Windows 2003 增加了一些访问控制及限制,且在系统默认配置下这些访问控制是允许使用的。然而,Windows 2003 以前的一些原有的系统已迫使其环境中应继续支持匿名连接。

2. Mac OS X 系统

Mac OS X 是苹果公司在它的 Intel 平台的 PowerPC 产品线上使用的基于 BSD 的 UNIX 的操作系统。

Mac OS X 由多个不同的组件组成，其中每个组件都潜在不同的安全漏洞。在过去几年中所发现最致命安全漏洞集中在以下 6 个方面：

① safari。

safari 是最近推出的 Mac OS X 版本所安装的默认的网页浏览器。浏览器中的漏洞将导致攻击者能够完全控制用户浏览器或登录会话。

② 图像 IO。

系统或应用程序使用的图像处理框架。在该处理框架中的漏洞可能涉及许多使用该处理框架的应用程序。通常，应用程序认为图像文件是“安全”的，在默认情况下，系统在不经提示用户的情况下，自动打开图像文件。

③ UNIX。

Mac OS X 是基于早期的类 UNIX 系统，并从中吸收了大量的 UNIX 系统代码。许多为 UNIX 或类 UNIX 系统而编写的应用程序运行于 Mac OS X 系统上，并随苹果机的 Mac OS X 操作系统一起发布，因此，Mac OS X 系统应用程序的漏洞补丁程序晚于 UNIX 系统上的漏洞补丁程序发布。

④ 无线连接。

Mac OS X 系统无线网络连接子系统中存在致命安全漏洞，离漏洞系统较近的攻击者可以利用该漏洞完全控制系统。即使被攻击的系统与发动攻击的系统并不属于同一逻辑网络，攻击者也能够利用该漏洞攻击系统。此外，在蓝牙无线接口子系统中发现了同样的问题。

⑤ 病毒/木马程序。

在 2005 年第一次发现在 Mac OS X 系统中存在病毒及木马程序。

⑥ 其他。

其余是一些不能明确界定类别的漏洞。

3. UNIX 系统配置缺陷

大多数 UNIX/Linux 系统的默认安装将安装一些标准的系统服务程序，对这些服务程序，即使安装了相应的补丁程序，也可能会造成意想不到的信息泄露。具有安全意识的系统管理员将通过关闭不必要的服务和/或使用防火墙保护从互联网访问这些服务，从而起到加固操作系统的目的。

例如，RedHat 企业版 Linux 系统默认安装了 cups(Common UNIX Printing System)，portmap(RPC support)，sendmail (Mail Transport Agent)及 sshd (OpenSSH server)等服务程序，而这些服务程序在确认没有使用必要时，应予以关闭。

特别令攻击感兴趣的是针对命令行程序发起的蛮力攻击，例如 ssh，ftp 和 telnet，由于这些服务提供远程访问，所以它们是攻击的目标。但近些年来，攻击者一起努力试图使用蛮力攻击的方法攻破这些应用程序所使用的口令。他们在不断增加的蠕虫及蝇蛆

(Bots)程序中加入了蛮力口令攻击引擎。系统中具有弱口令强度的用户账号及易攻破，并由此提升权限至超级用户的访问权。root-kits 就是一套攻击者攻入系统后，隐藏在系统中，用于发起进一步攻击系统的套件。对我们来说，重要的是必须切记：蛮力攻击口令是一种攻破已安装了系统补丁程序的操作系统的技术。

具有安全意识的系统管理员使 SSH 作为他们远程交互操作的方法。如果 SSH 版本是当前最新版本，且已安装了补丁程序，那么该 SSH 服务本身可以认为是安全的。然而，无论是否是最新版本及更新了补丁程序，该系统都能通过蛮力口令猜测攻击攻破。对于使用 SSH 服务，建议使用公钥身份鉴别方式来避免此类攻击。对于其他的远程交互服务，建议审计口令的强度，保证它们足够复杂，用以防止蛮力攻击。

15.2 系统平台的安全加固

平台加固是一种用来分析和确定操作系统及服务程序弱点，并引入适当的更改以保护操作系统及其服务程序免受攻击的方法。平台加固可以帮助检查操作系统的各个组件及相关应用程序，以确定最安全的配置方案。配置过程包括从系统中删除不需要的服务、软件和用户，加强对操作系统工具和软件的控制。最终结果是有了一个在自身安全方面扮演积极角色的平台，该平台不仅仅依赖于外在的安全机制。

15.2.1 系统平台的加固方案

尽管加固系统平台的具体方案是依据系统平台的不同而定的，但总体指导思想是一致的，具体如下：

① 减小无用软件、服务和进程的数目。

② 在持续提供对资源的访问的同时，要使所有软件、服务及进程配置处于最安全的状态。

③ 尽可能避免系统对其身份、服务及功能等信息的泄露。

为达到成功加固系统平台的目的，应采取如下步骤：

① 确定目标系统的用途。

② 评定系统是否符合最初要求。

③ 根据目标系统需求，制定安全策略。

④ 采用标准构件的方法实施系统平台加固。

1. 确定目标系统的用途

逐一确定每个目标系统的用途，确保不要遗忘任何系统平台。对企业最危险的安全威胁之一是仍起作用却被遗忘的系统平台。那些原以为被取代的系统，实际仍然起作用，并作为执行未经授权动作的主机，是企业最危险的安全威胁。在加固平台时，必须回答下列问题：

① 为什么要建这个平台？

② 谁对这个平台负责？

③ 这个系统能满足与业务相关的需求吗？

④ 要满足这个需求需要哪些服务？

⑤ 谁需要访问这个系统？

⑥ 这个系统需要访问什么资源？

这个列表反映出在使用系统之前必须编辑的需求文档的类型。它既作为对系统生存周期有关过程的健全性检验，又定义了系统必需的应用程序、服务和进程的蓝图。

2 评定系统是否符合最初要求

一旦确定了系统需求，下一步就是评定系统以确定实际的实现是否符合最初的需求。这个评定不需要使用复杂的方法和工具。系统操作员通常可以提供服务、端口、应用程序、软件版本、用户及进程的清单。这个简单的清单通常足以建立一个简单的评测报告。很多情况下，实际服务的数量远远大于所需要的服务数量。此信息将作为下一阶段工作的基准。

3. 根据目标系统需求，制定安全策略

要设计一种策略以满足目标系统平台的需求，通常，安全策略的制定应考虑以下 5 方面的内容。

（1）网络

这个系统正常运行需要多少网络访问量？用户需要对系统进行远程访问吗？这个访问是源自于网络可信的部分还是不可信的部分？组织会支持取消所有未加密的访问服务吗？来自这个系统的文件需要和别的系统共享吗？这个系统能进行远程管理吗？防火墙或数据包过滤设备会保护网络访问吗？如果不能，我们能在平台上实现数据包过滤吗？如果能，防火墙能够支持预期的系统吞吐量吗？

（2）系统软件

该系统在最近是否发布了标准软件版本或补丁？这些软件版本是否符合供应商推荐的安全补丁等级？有没有不再使用并可以卸载的主要内部软件包？是否使用了基于菜单或 GUI 的管理程序？关键的软件组件是否存有正确的日志？这些日志是循环的还是会归档？是否使用标准的图像来建立新的系统以保持一致？

（3）文件系统

文件系统是本地的，还是有远程的装入卷？这些远程装入卷是否使用安全协议？本地卷是否正确划分了分区？日志是否会超出其存储空间并损坏系统？是否使用了基于操作系统的加密技术来保护文件？可执行文件是否受到合理限制？SUID(Set User ID)的功能是否受限于关键的可执行文件？系统是否正确地备份？

（4）用户

哪些用户需要系统的访问权？他们是否使用了强密码？密码是否有期限要求？账户的储存和管理是本地的还是使用一个公用目录？用户账户是否被定期审核和重新验证？谁能创建账户？基于角色的账户能否执行特权功能？是否对使用进行了监控？是否设置了用户路径和权限集？

（5）物理

系统是否位于安全的数据中心？它是否连接到安全的电源？是否有合适的温度调控

系统？系统控制台是否置于锁好的机柜里？控制台在处于不活动状态一段时间后是否会自动退出系统？

4. 用标准构件的方法实施系统平台加固

在实施系统平台加固的最后过程中，应采用构件的开发方法以保证加固成功。标准构件是一种具有达到特定目标所需的全部功能的特定系统类型的每个小部件集合的镜像。企业可以为桌面、Web 服务器、数据库系统及用于企业的所有其他类型平台开发配置文件。这些配置文件指定了操作系统的类型、补丁级别、应用程序软件及安全设置。然后在实验环境中对它们进行研究，并镜像为一种可以重复生产的形式，这样可缩短生产时间，因为所有软件和配置都包含于这个镜像中。当新的补丁和需求及软件版本出现时，配置文件和图像必须进行更新。

标准构件也可用于简化现有系统的加固。很多情况下，可以实现交换系统（Swap-Out System）。有了交换系统，可以将标准构件映射到相应的硬件平台上。目标系统的配置和数据在替代系统上执行，然后将两个单元进行交换。在最后一步中，数据进行了同步化，产生了符合所需操作目的的生产平台，不同的是，这是一种更为安全的方式。随后旧的单元可以重新映射以取代另一个生产系统，然后反复重复整个过程。通过使用这种方式，能够节省时间和资源，从而实现更为有效的安全组织。

15.2.2　系统平台的加固指南

依据平台加固的总体指导思想，平台加固应从以下几方面考虑。

1. 端口和进程

网络操作系统使用进程向外提供服务，减少无用软件及服务的任务就是要在所有系统进程中找出多余进程。由于进程通过打开网络端口向外提供服务，所以找出多余进程的最快方法是观察进程及端口对应表。

netstat 是列出一个系统上所有打开的 TCP/IP 网络端口的命令，通过该命令，可以找出系统平台上的所有打开的监听端口。这些打开着的端口正是入侵者所要攻击的，因为它们通向系统平台内部。因此，作为平台加固的一部分，我们使用 netstat 命令来识别出无关端口，并由此找到需要删除或需要禁用的服务。图 15-1 显示出，主机 192.168.5.102 开放了 Telnet、SSH 和 FTP 等服务。

禁用 Windows NT/2000 中不必要的服务非常简单，具有图形界面的控制面板可以用来设置各项服务并确定它们如何启动，只需要浏览列表来关闭或禁用不需要的服务。图 15-2 显示了 Windows 2000 的服务面板。

禁用 UNIX 平台上的服务要复杂一些。主要是 UNIX 版本服务的启动脚本及文件的存放位置不同。对于每个要启动的服务，操作系统中通常包含一组启动及停止脚本，启动时操作系统按所需的顺序调用这些脚本，关闭时系统执行停止脚本。加固过程中要合理定位不同操作系统脚本的位置并合理禁用不必要的服务程序。表 15-1 列出了一些 UNIX 系统启动脚本的位置。

```
[zwg@zwg-HR9 zwg]$ netstat -na
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0    138 192.168.5.102:23        192.168.5.35:3755       ESTABLISHED
udp        0      0 0.0.0.0:701             0.0.0.0:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  5      [ ]         DGRAM                    866    /dev/log
unix  2      [ ACC ]     STREAM     LISTENING     1038   /dev/gpmctl
unix  2      [ ACC ]     STREAM     LISTENING     1091   /tmp/.font-unix/fs7100
unix  2      [ ]         DGRAM                    1053
unix  2      [ ]         DGRAM                    996
unix  2      [ ]         DGRAM                    877
[zwg@zwg-HR9 zwg]$
```

图 15-1　netstat 命令输出示例

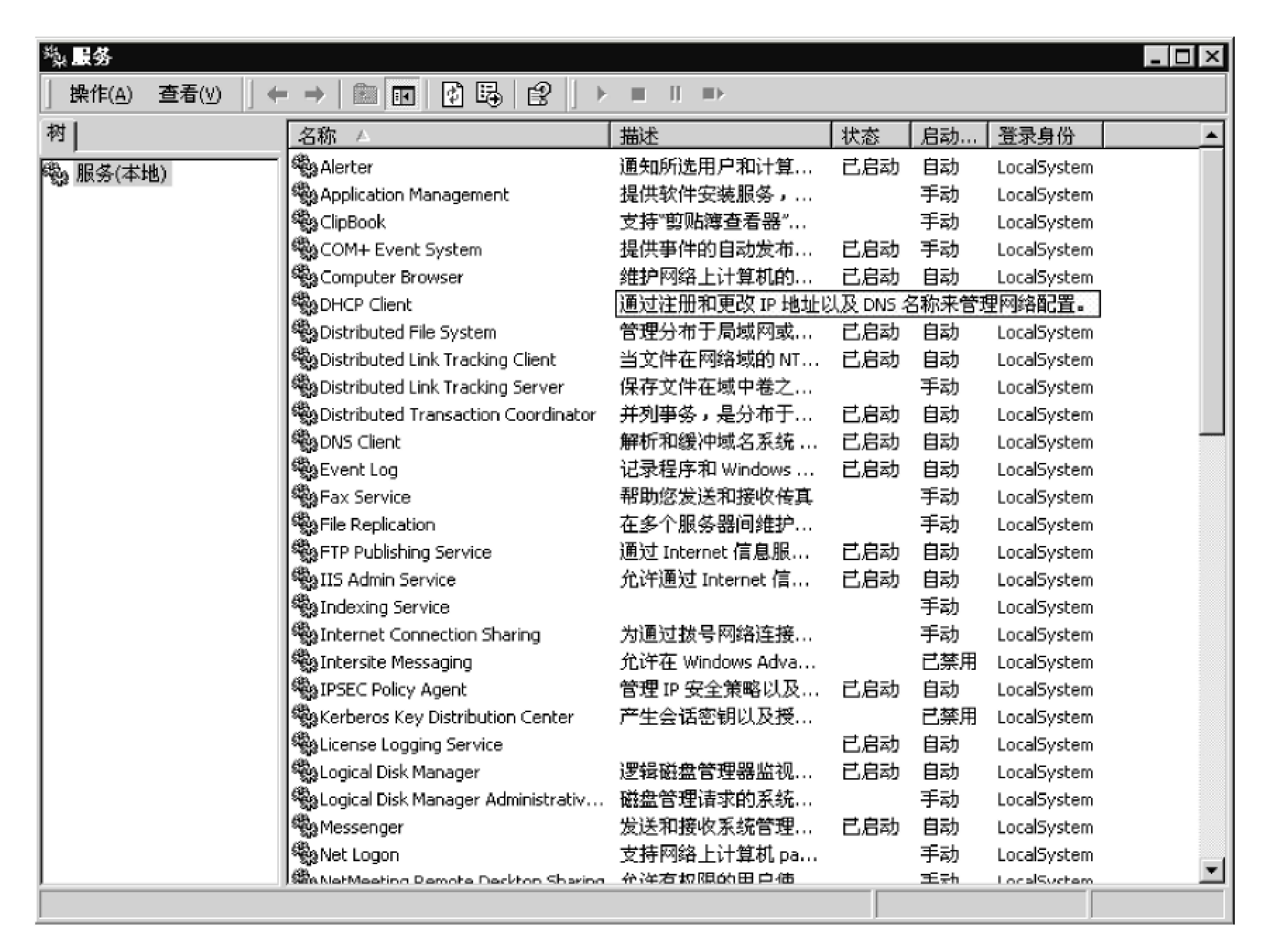


图 15-2　Windows 2000 服务面板

表 15-1　不同版本 UNIX 启动脚本的位置

操 作 系 统	启动脚本位置
Solaris	/etc/init. d
Linux(redhat、turbo Linux)	/etc/rc. d/init. d
FreeBSD	/etc/rc. init

2 安装系统补丁

所有软件都有缺陷。为了修复这些错误，供应商会发布软件补丁。如果没有这些补丁，组织可能就会容易遭受攻击。在有很严格的更改控制策略的组织中，及时安装补丁会

是一个问题。对补丁的彻底测试是这个过程的关键部分，因为供应商在解决旧问题时，有可能会引入新的问题。而对于和安全缺陷无关的补丁来说没有问题。但是，入侵者搜索和利用安全弱点的速度要求有更快的安全补丁修正过程。企业必须注意安全补丁的发布，并随时准备快速地使用它们。建议企业及时查阅 www.sans.org 以获得最新漏洞修复信息。不同操作系统的系统补丁如表 15-2 所示。

表 15-2 不同操作系统的系统补丁

操作系统	补丁类型	安装方式	如何获得
Windows NT/2000/XP/2003/Vista	Hotfix、服务包	自安装	update.microsoft.com
Solaris	单或多个补丁	instllpatch	Sunsolve.sun.com
Linux （Redhat、Mandrake 等）	替代软件包	Rpm-u	www.redhat.com/apps/support/errata www.mandrakelinux.com
NetWare	NLM	Patch	support.novell.com/filefinder/6385/index
FreeBSD	新的源代码	重新编译新代码	www.freebsd.org

3. 密码强度及存储

计算平台速度的巨大改进及人们对现代密码系统的兴趣和理解的增加，向平台安全提出了新的挑战。UNIX 系统传统上使用一些快速类型的哈希算法来对所存放的用户密码进行加密。为了允许低特权进程使用这个密码系统，密码存储（依赖于加密技术来保护它）需要全局性的可读许可。

系统允许的密码强度是传统 UNIX 系统的另一薄弱之处。密码强度取决于密码中使用的字符数和随机性。例如，3D8%de 的强度就比 dog 要大得多。

越来越快速的计算机和可以免费得到的解密软件已经使密码存储越来越容易受到离线攻击，因为几乎任何用户都可以访问用户口令的密文。现代的 PC 有足够的能力解密这些脆弱的口令。

UNIX 系统能够为用户口令存储添加保护层，只需要设置这些系统就可以了。现代的 UNIX 系统（甚至一些合理修补的遗留系统）对无特权用户隐藏了用户口令的密文，但是仍然允许他们访问认证子系统（称为阴影）。它们也可以阻止用户使用容易被猜测到的字典词汇作为用户口令并要求用户定期更换口令。UNIX 系统有一些固有的对用户透明的功能，只需要激活它们就可以了。

Windows NT/2000 也包含了保护本地密码存储完整性的方法。通过一次性使用 syskey 命令，可以使操作系统在密码存储中使用更强的加密技术。Windows NT/2000 也可以要求用户使用经常更改的更长、更随机的密码。

4. 用户账户

用户账户标识了需要访问平台资源的实体（无论是应用程序进程还是人）。操作系统通过权限和优先权将用户账户与其访问控制系统相关联。因为用户账户是合法进入系统

的机制，所以入侵者常常试图利用用户账户管理和访问控制中的缺陷。如果可以作为合法用户轻松地登录系统，那么为什么还要浪费时间去做自定义缓冲器溢出攻击呢？

用户账户管理的弱点有 5 个方面：弱密码、制造商默认的账户、基于角色的账户、公司默认账户，以及废弃账户。在所有情况下，平台加固的目标是将用户账户数目减少到所需的绝对最小值。下面描述了用户账户管理 5 个方面的缺点：

- 在前面的小节中已经讨论了关于弱密码处理的问题。
- 制造商默认的账户由制造商创建，是为了维护或者在安装时首次登录到平台而使用的。虽然今天已经不太流行，但是这些账户仍然存在于一些旧的系统上，这可能会非常危险。
- 基于角色的账户非常危险，因为它们不能实现适当的可信赖性。角色账户由一群人来使用，而不是要求用户使用他们自己的 ID 登录。例如备份操作员或者 Web 站点管理员。
- 公司默认账户是由于标准构件过程的误用而安装于整个企业平台上的账户。这些账户和基于角色的账户的相似之处是，它们不能实现适当的可信赖性。然而，它们可能会更危险，因为它们错误地允许一些用户匿名登录到系统中。
- 废弃账户会导致最糟糕的问题，因为它们的存在导致了安全规程极危险的缺陷。最佳实践证明，不再被授权访问资源的用户或者那些离开公司的用户，他们的账户应当立即停止使用，废弃的账户最容易受到同事和支持人员的内部攻击。

关于用户账户管理需要在平台加固时关注的另一个方面是，那些用于运行人机交互式进程（例如 Web 服务器）的用户账户。默认情况下，这些进程的绝大部分以超级用户特权运行，这意味着任何对这些进程的成功攻击将获得对系统访问优先权的极大提升。只有关键的系统和核心任务，虽然需要比较高的访问级别，但是其他的应用程序并不需要。应该创建和配置应用程序所需的确切访问级别的专用用户账户，以帮助保护系统，不让入侵得逞。这些措施包括锁定账户的远程登录权利或者禁止获得对 Shell 提示符的访问，还包括限制账户只能访问自己的文件。

5. 用户特权

用户特权是 UNIX 系统安全的基础之一。正确实现的用户特权应该确保用户只具有他们执行任务所需要的访问权限。UNIX 系统中的超级用户是一个享有完全和不受限系统资源访问权的用户账户。这个账户是为专门需要高级别访问的系统管理任务保留的，但是系统管理员常常将之用于他们普通的日常活动。大多数 UNIX 系统不提供一个中间级别的系统特权，所以超级用户特权往往被授予比完成任务实际所需的数目多得多的用户。因为超级用户账户可以破坏和修改系统安全功能，所以系统管理员每次给予这个关键的访问级别，就是在增加系统被攻击的可能。并且，由于只有一个超级用户账户，所以要跟踪谁在使用它是很困难的。

SUDO（Set User and Do）设计使系统管理员能够给超级用户更精细级别的访问权。可以为每一个用户指派通常只能作为超级用户运行的特定的应用程序和功能，而不是真正地使用超级用户账户。SUDO 也可以启用详细的日志记录，使得可以根据任何运行于

SUDO 的超级用户功能追踪到某个特定的用户。在特定的应用中，使用 SUDO 意味着没有人使用过超级用户账户。

6. 文件系统安全

通过在程序文件上设置 SUID 标志，某一个进程可以临时提升其特权用以完成某项任务(例如文件 passwd)。当程序执行时，可以暂时得到这些额外的特权而不用被全时授予如此高的特权。这个 SUID 标志常常过度使用，当它与被黑客修改过的软件包结合时，被修改的程序执行后会使某个用户得到全时提升的系统权利。UNIX 系统可能有很多带有这个标志的组件，但是通常只需要它们中的一小部分。建议使用命令从整个系统中删除不需要 SUID 标志程序的 SUID 标志。

7. 远程访问的安全

Telnet 和 rlogin 是 UNIX 系统上最常用的远程访问方式。这些系统都不采用加密技术来保护远程访问会话。一种被动的网络监听攻击可以观察用户在进入 Telnet 或者 rlogin 会话中按下的每一个键。安全 Shell (Secure Shell，SSH)是一种在 UNIX 及 Windows NT/2000 系统上使用的软件包，它提供与 Telnet 和 rlogin 相同功能，但增加了加密会话功能。这个软件包已经成为用加密和访问控制的各种可配置级别进行安全远程访问的行业标准。

8. 服务标题、操作系统指纹

我们已经提到过，平台加固要减少系统泄露的信息数。默认情况下，像 telnet 和 ftp 样的服务在被访问时，会显示一个描述其软件版本和平台类型的标题。攻击者使用这个信息，通过检查任何含有关于特定软件版本和类型的可利用信息的数据库，可以确定该平台是否有可利用的漏洞。许多入侵者通过扫描 Internet 的整个区段，寻找他们已知可利用的服务的特定版本漏洞。这个服务信息对平台的正常运行完全是不必要的，因此完全可以将之删除。这样，攻击者就只能盲目地攻击服务了。

另外一个对攻击者特别有用的是系统平台的指纹信息。通过使用特定的工具查询系统的网络服务，入侵者可以将结果与属性数据库相匹配，以确定操作系统的类型和版本。这样，攻击者可以使攻击针对特定操作系统的弱点。通常，应把这种指纹信息伪装成其他操作系统，或者可以伪装成不与任何操作系统相匹配。与服务标题一样，做这种修改不会影响平台的正常功能，而且可以大大增强防御能力。

15.2.3 系统平台的加固工具

加固工具是一种自动高效地帮助人们确定系统平台的漏洞，并辅助人们加固系统平台的工具。目前常用的加固工具主要有以下几种。

1. nessus

nessus 是一个功能强大而又免费的网络漏洞扫描工具，运行于 POSIX 系统(Solaris、FreeBSD 和 GNU/Linux 等)。该系统被设计为客户端/服务器模式，服务器端(nessusd)负责进行安全扫描，客户端(nessus)用来配置、管理服务器端。nessus 在进行漏洞扫描时

不仅根据端口号来判断服务类型，还能够检测出开设在非标准端口的常见服务类型，并根据其版本号进行相应的漏洞检测。nessus 扫描结果可以保存为多种文件格式，并且对每种扫描出的系统漏洞给出建议的加固方法。

2. HardenNT

HardenNT 是专为 Microsoft Windows 系统平台设计的众多加固脚本之一。尽管它的设计是针对 Windows NT 的，但它的主要功能同样适用于 Windows 9x 及 Windows 2000。

HardenNT 主要完成以下工作：

- 根据操作系统版本及 CPU 的结构安装相应的安全补丁；
- 限制用户组的默认 NT 特权；
- 启动 Windows NT 安全事件审计服务；
- 设置 NTFS ACL 许可，删除/移走重要的安全文件；
- 保护 Windows 系统的注册表。

3. YASSP

YASSP 是一个用于 Solaris x 系统安全加固的包。它设计同 Solaris 安装过程一起运行。它的目标是建立一个面向 Internet 的平台(例如 Web 服务器、Ftp 服务器)，但是也可以用于内部系统。YASSP 完成如下安全设置：

- 禁止无用网络服务；
- 解决文件属性及保护弱点问题；
- 启动系统日志审记；
- 调整重要系统参数，禁止堆栈区执行代码。

YASSP 的配置通过 yassp.conf 文件完成。在这个文件中，用户指定希望 YASSP 处理哪个文件。其中可能包括删除初始化文件或者添加可以增强基本安全功能的目录。

4. titan

titan 由信息安全的先驱者 Brand M. Powell、Dan Farmer 和 Matthew Arch 开发。它由一系列可配置的 shell 脚本组成。用户可以在诸如文件权限和根目录等属性上做低级的配置更改。由于采用 shell 脚本编写，具有良好的扩展性及移植性，所以 titan 可以在多种 UNIX 版本上运行。

人们为 titan 编写了许多模块，每个模块实施一个特定配置的更改。下面是其中一些模块的例子：

- 禁用自动装入器；
- 设置 Solaris BSM(Basic Security Module)来审核系统事件；
- 设置公共桌面环境以忽略危险的外部连接；
- 登录时，加强所有用户的默认权限；
- 确保默认的系统账户不会被攻击；
- 删除不必要的 SUID 配置；
- 禁用不严格的信任关系。

所有这些模块都有完备的文档，并为用户提供关于其功能的简要描述。

5. LC4

LC4 是针对 Windows 系统平台的密码审计及恢复工具。LC4 功能之一是以在线或离线方式检测 Windows NT/2000 系统的用户密码强度。其网络窃听功能窃听所有 SMB 会话，用以发现其他系统用户密码的弱点。

6. tcp 封装器

运行于 UNIX 系统上的 tcp 封装器(tcp wrapper)，完成对系统的 tcp 输入请求实时监视，若发现是其负责管理服务的连接请求(如 telnet、ftp、finger、rwho 和 tftp 等，定义在 inet. conf 中)时，首先进行一定的验证(如通过 host. allow、host. deny 等配置文件)，当通过验证后，启动原真正的服务器进程，如 in. ftpd 或 in. telnetd 等对连接请求进行处理。

7. Tripwire

Tripwire 是一种数据完整性检测工具。它是由 Purdue 大学 COAST 实验室的 Gene H. Kim 和 Eugene H. Spafford 于 1992 年开发的。它们的目的是建立一个工具，通过这个工具监视一些重要的文件和目录发生的任何改变。1997 年，Gene H. Kim 和 W. Wyatt Starnes 发起成立了 Tripwire 公司。他们成立这个公司的目的之一是发布一个能够用于更多平台的商业升级版本 Tripwire。

Tripwire 采用的技术核心就是对每个要监控的文件产生一个数字签名，保留下来。当文件现在的数字签名与保留的数字签名不一致时，那么现在这个文件必定被改动过了。具体到监控项目，在 Tripwire 的配置文件中说明。

15.3　UNIX 系统安全

15.3.1　系统设置

本节所述 UNIX 系统设置主要是与安全相关的内容，是对不同厂商 UNIX 系统设置的抽象浓缩，所以不涉及具体命令，相关内容请查阅相应 UNIX 系统管理员指南。

1. 安装系统补丁及其他重要的安全软件

(1) 安装最新补丁程序

安装 UNIX 系统后，首先要做的工作是安装操作系统补丁程序，补丁程序是操作系统厂商根据系统安全漏洞(CVE)对操作系统所做的修改，它对系统的安全及可靠性是至关重要的。

(2) 重要的安全软件

① SSH。在 SANS/FBI 公布的 2003 年 10 大 UNIX 安全漏洞中，ftp 及 telnet 会话用户名及密码等敏感信息以明文传送名列其中。SSH 协议解决了登录及文件传输会话安全加密问题，OpenSSH 是一个免费且符合 SSH 协议的软件包。

② TCP Wrapper。TCP Wrapper 允许系统管理员通过远程连接的 IP 地址来控制谁能够访问系统提供网络服务。通过使用系统的 Syslog，TCP Wrapper 能够记录下所有成功及未成功的连接。

2. 将 inetd 提供的网络服务减至最小

最小化网络服务，如果有可能去掉 telnet、ftp、tftp、rlogin/rsh/rcp 及与 X 窗口相关的守护进程，该项工作与 UNIX 版本有关，在 Solaris 系统中为编辑 inetd. conf 文件。

3. 最小化系统启动后所提供的应用服务

如果没有绝对的必要，应关闭以下服务：串口登录服务、邮件服务、基于 Windows 系统的 Samba 服务、NFS 服务器及客户端进程、RPC 服务、目录服务、打印机守护进程、Kerberos 服务、X 服务、Web 服务器、SNMP 服务、DHCP 服务、DNS 或 NIS 服务及路由守护进程。最后应设置系统守护进程正确的 umask 为 022。

4. 系统核心参数的调整

通过调整核心参数来达到加固系统平台的目的。具体参数根据系统的不同有很大差异。通常，核心参数包括：

① 禁止系统转储核心文件；

② 禁止堆栈执行代码，防止缓冲区溢出；

③ 修改网络参数，例如，在 Solaris 系统中使用 ndd-set 命令修改/dev/ip 及/dev/tcp 等参数，在 Linux 下，使用 echo 命令修改/proc/sys/net/ipv4 目录中的参数。具体每个参数的名称及功能需查阅相应 UNIX 系统提供商所提供的系统管理员指南。

5. 加强日志功能

为了跟踪系统的各种活动，及时发现各种攻击及出现问题后处理，安全专家建议应加强系统的日志记录功能。为了保证系统安全，应对下面事件进行记录：

- LOG_AUTH。用于记录用户所有成功或失败的系统登录请求；
- ftp 服务连接信息；
- 当必须要使用 ftp 服务时，要启动 ftp 服务连接跟踪日志功能；
- 启用所有 cron 活动的日志；
- 确认所有系统日志文件的访问权限为 664，及文件的属性及同组用户具有写权限。

6. 文件及目录访问许可权设置

确认所有重要系统文件及目录的访问许可权，需要确认的文件如下。

（1）以 ro/nosuid 方式 mount 文件系统

确认除系统文件所在卷及一些必要程序所在的卷外，其他卷以 ro/nosuid 方式 mount，以防恶意程序执行 suid 操作。Solaris 系统是修改 vfstab 文件，Linux 系统是修改/etc/fstab 文件。

（2）设置关键文件访问许可

通过以下命令设置关键文件访问许可权：

```
chmod 644 passwd group
chmod 400 shadow
```

(3) 在任意账号可写的临时目录上设置粘贴位

通过使用命令 chmod +t dir-name，可在任意账号可写的临时目录上设置粘贴位，以防某用户有意或无意重写其他用户创建的临时文件。其中 dir-name 表示目录名。例如：

```
chmod+ t/tmp
```

(4) 找出非授权的 SUID/SGID 执行程序

系统管理员有责任找出所有系统中存在的非授权的 SUID/SGID 执行程序。以下命令用于找出系统所有设置 SUID/SGID 的程序。

```
find/-type f\(-perm-04000-o-perm-02000\) - print
```

7. 系统访问、身份鉴别及授权

(1) 删除/etc/pam. conf 或/etc/pam. d. rhost 中的. rhost 支持

在使用 BSD 的 R 系列命令(rlogin、rsh、rcp)时，. rhost 文件实现了基于远程网络地址或主机名的弱身份鉴别，潜在的攻击者是非常容易伪造网络地址及主机名的。删除. rhost支持可防止系统免遭此类攻击。Solaris 系统下的命令脚本是：

```
cd /etc
grep - v rhost_auth pam.conf> pam.conf.new
mv pam.conf.new pam.conf
chroot root:sys pam.conf
chmod 644 pam.conf
```

(2) 建立/etc/ftpuser 文件

ftpuser 文件列出了不能够通过 ftp 访问系统的用户清单。通常，仅允许普通账号的用户能够通过 ftp 访问系统，而系统账号，如 root、daemon、bin、sys、adm、lp、uucp 和 smmsp 等应禁止。

(3) 禁止 X 服务器监听 tcp 6000 通道

X 服务器通过监听 tcp 6000 通道的请求来向远程 X 客户提供服务，由于 X 窗口使用了相对较弱的身份认证协议，攻击者可以未经授权地访问本地 X 服务器，从而暴露系统敏感信息。管理员应使用 nolisten tcp 选项来禁止 X 服务器监听 tcp 通道 6000 的服务请求。

(4) 设置屏幕保护

当使用 X 窗口时，应设置屏幕保护，同时设置需要使用口令来恢复 X 窗口会话。

(5) 严格限制使用 cron/at 用户

cron 及 at 命令用于定时执行系统命令，在某些 UNIX 系统中，cron 及 at 以超级用户身份执行。cron. allow 及 at. allow 列出了允许使用 cron 及 at 的用户名。

(6) 限制以 root 身份登录到系统控制台

除非在紧急情况下，否则禁止使用 root 账号登录系统。通常，系统管理员应通过使

用非特权账号及一些授权机制(例如 su 命令)来获得普通账号以外的权限。Solaris 系统为修改/dev/console 文件,Linux 系统为修改/etc/securetty 文件。

8. 用户账号及环境

系统管理员在正常情况下应设置的项目如下:

(1) 锁定系统账号。系统管理员应锁定非普通用户的账号。通过查询文件/etc/passwd 可以找到所有要锁定的系统账号。例如 daemon、bin、sys、adm、lp、uucp 和 smmsp 等情况根据系统及安装程序不同而变化。使用命令为:

```
passwd-l user-name
```

(2) 确认是否有无口令的账号。使用如下命令显示无口令的账号:

```
awk - F:'($ 2== "") {print $ 1}' /etc/shadow
```

(3) 确认除 root 账号以外,没有 UID 为 0 的账号。UID 为 0 的账号具有超级用户权限。使用下面命令显示 UID 为 0 的账号:

```
awk - F:'($ 3== 0) {print $ 1}' /etc/passwd
```

(4) 确认 root 的当前路径及路径 PATH 指定路径的 root 组可写目录中文件,以防植入木马程序。

(5) 保证用户起始目录正确权限设置。组用户或任意用户可写用户起始目录的属性,很有可能使一些恶意用户利用,用以窃取或修改受害用户数据,以至于得到用户权限。应使用以下脚本修改用户起始目录权限为 750 或更加严格。

```
for dir in'awk - F:'($ 3>=500) {print $ 6}' /etc/passwd'
do
    chmod g-w $ dir
    chmod o-rwx $ dir
done
```

注意:其中 500 表示系统分配给普通用户的最低 UID,该值取决于 UNIX 系统。

(6) 删除用户起始目录中的.netrc 文件。该文件包含了 ftp 客户自动登录到 ftp 服务器所用的用户名及口令等敏感信息,且这些信息以明文存放。使用以下脚本自动删除所有用户起始目录中的.netrc 文件:

```
for dir in 'cut - f6 d: /etc/passwd'
do
    rm - f $ dir/.netrc
done
```

(7) 设置默认用户 umask 位。umask 位表示用户建立文件的默认读写权限。正确的读写权限可以防止用户的敏感信息被窃取、修改及账号泄露。umask 077 表示用户所创建的文件不能由其他用户读、写及执行,而 umask 022 则表示用户所创建的文件对系统中其他用户只开放读权限。设置 umask 位的方法是,在标准的 shell 构成文件中(依不同的

UNIX 及 shell 而定，例如，Solaris 系统下使用 B shell 时的构成文件为用户起始目录下的.profile 文件)插入一条 umask 命令。

15.3.2　用户管理

UNIX 系统用户分为两类，一类称为系统用户，这是给系统管理员等对系统特殊要求的用户使用的。这类用户具有某些特权，其中以超级用户(root)权限最高，root 账号在系统安装时创建。另一类用户是普通用户，一般的系统使用者都是系统的普通用户，这类用户由系统管理员创建。用户管理主要是指管理员对普通用户的创建和删除、修改用户口令、暂停某账号使用、修改用户属性等日常维护工作。

15.3.3　系统管理

系统管理是由系统管理员完成的一项复杂的日常工作。通常，系统管理员要完成的工作包括启动系统、停止系统运行、安装新软件、增加新用户、删除老用户、端口服务管理、打印服务管理、文件系统维护、数据备份与恢复、网络系统管理、系统性能维护，以及完成、保持系统发展和运行的日常事务工作。

系统安全管理的主要内容如下：

- 防止未授权存取；
- 防止泄密；
- 防止用户拒绝系统的管理；
- 防止丢失系统的完整性。

15.4　Windows 2000 服务器安全

1. 系统设置

(1) 安装系统补丁

Microsoft 补丁程序分为 3 种类型：

① Service Pack。

Microsoft 原计划几个月发布一次，包括至发布之日止系统全部大小 bug 修补。

② Hotfix。

及时发布的每个小的系统 bug 的修补，有时甚至在发现系统 bug 数小后即可发布，基本上是发现一个 bug，发布一个 hotfix。

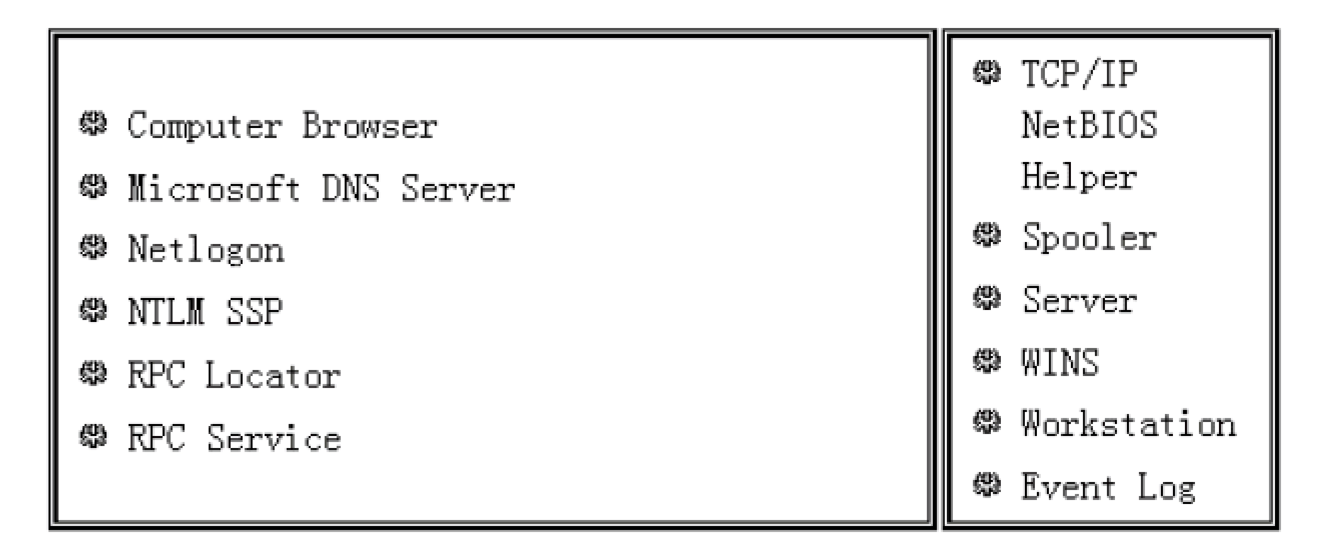
③ Hotfix Rollup。

周期性地发布，它是 hotfix 的累计。其中安装①、③所述补丁是在系统安装完成后做的第一项工作，而安装②所述补丁是日常系统维护中要做的工作。

(2) 最小化系统服务

按下列步骤进入服务管理菜单，逐项审核服务，关闭不需要的服务：依次选择“开始”→“设置”→“控制面板”→“服务”命令。

Windows 2000 Server C2 级别安装的默认服务：



(3) 文件系统设置

确保所有磁盘卷格式化为 NTFS 文件系统。

2. 账户策略

必须加强账号管理。建立账号策略为：密码最短存留期 1 天、密码最长存留期90 天、密码长度最小值 8 个字符、启用密码符合复杂性要求、强制记住密码使用历史为 24 个、停用可还原的加密密码存储方式、账户锁定时间大于 15 分钟、账户锁定阈值最多 3 次、复位账户锁定时间大于 15 分钟。

3. 审计策略

审计策略实现对系统和计算机状态的追踪和记录。通过对这些记录的管理，系统管理员可以明确系统的运行情况，在出现问题的时候，能够及时进行问题分析，快速处理和解决。应建立审计策略：审核账户所有成功和失败用户登录事件(本地账户及域账户)、审核所有成功和失败账户管理事件、审核特定对象的失败访问、审核所有尝试修改用户权限及策略的行为、审核特权使用、审核系统成功和失败事件(包括计算机的启动与停止)、所有日志文件必须大于 80M、禁止 guest 账号访问日志文件、日志覆盖方式选择按照需要改写事件的方法。

4. 配置安全选项

通过配置系统安全选项，增强系统安全性。需要配置的安全选项为：禁止匿名访问、禁止服务器操作员计划任务、禁止在未登录前关机、只允许 Administrators 卸载或弹出可移动 NTFS 媒体、在挂起会话前所需要的空闲时间大于 30 分钟、根据需要开启审计对全局系统对象的访问及备份和还原权限的审计日志、当登录时间用完时自动注销用户登录(本地及域用户)、系统关闭时清除虚拟内存页面文件、为尽量提高通信的安全性，当协商可以使用安全通信的时候，使用安全的数字签字通信、用户必须按 Ctrl＋Alt＋Delete 组合键登录系统、不显示上次登录用户名、LAN Manager 身份验证级别应为 NTLMv2、实现必要的安全告知、可被缓冲保存的前次登录个数为 0、允许更改机器账户密码、禁止用户安装打印机驱动、提前 14 天进行更改密码提示、故障恢复控制台禁止自动系统管理员级登录、故障恢复控制台禁止对所有驱动器和文件夹进行软盘复制和访问、重命名系统管理员账号 Administrators 为其他名字、重命名来宾账号 guest 为其他名字、只有本地登录的用户才能访问 CD-ROM、只有本地登录的用户才能访问软盘驱动器、尽可能使用安全的通信、禁止发送未经加密的密码到第三方 SMB 服务器、智能卡移除后锁定工作站、安

装未签名驱动程序或其他程序至少发出警告允许安装或不允许安装、禁用 Dr. Watson 故障记录、禁止系统调试器的自动运行、禁止自动播放磁盘媒体上的任何应用程序、禁止任何用户的自动播放功能、禁止自动登录、禁用拨入方式访问服务器、停用蓝屏后自动重新启动功能、禁用 CD 自动播放、删除服务器上的默认共享、保护计算机浏览器不被欺骗、防止源路由攻击、保护默认网关网络设置、确认 ICMP 最短路径路由、防止数据包碎片攻击、设置对活动连接的检查时间间隔为 5 分钟、设置参数以防恶意命名攻击、设置参数用以防范 SYN 洪泛攻击、设置 TCP 最大半连接数 100～500、设置 TCP 最大半连接丢弃数 80～400、启用 IPSec 保护 Kerberos RSVP 通信。

5. 服务安全配置

根据服务最小化的原则关闭一些不必要的服务，禁用一些存在安全漏洞的服务。对服务的配置为：禁用 Alerter，Clipbook，Computer Browser，Fax Service，FTP Publishing Service，Internet Connection Sharing，Messenger，Remote Registry Service，Routing and Remote Access，Simple Network Management Protocol (SNMP) Trap，Telnet，对于内部服务器禁用 Automatic Updates，Background Intelligent Transfer Service，如没有必要禁止使用 IIS Admin Service，NetMeeting Remote Desktop Sharing，World Wide Web Publishing Services。

6. 用户权限安全设置

本着最小化原则，通过依次选择“本地安全设置”→“本地策略”→“用户权限分配”命令，严格控制用户访问系统的权限。控制用户访问权限包括：控制 Users 及 Administrators 组中的用户通过网络访问本计算机、禁止赋予系统的管理权限到其他用户、禁止用户在域中加新的工作站的操作、限制只有 Administrators 才能完成文件及文件夹的备份操作、跳过遍历检查为 Users、更改系统时间为 Administrators、创建页面文件为 Administrators、创建标记对象为空、创建永久共享对象为空、调试程序为空、拒绝从网络访问本机器为 Guests、拒绝作为批处理作业登录为空、拒绝作为服务登录为空、拒绝本地登录默认为空、允许计算机和用户账户被信任以便于委任为空、从远端系统强制关机为 Administrators、生成安全审核为空、磁盘卷的维护任务由 Administrators 执行、增加进度优先级为 Administrators、装载和卸载设备驱动程序为 Administrators、内存中锁定页面为空、作为批处理作业登录为空、作为服务登录为空、允许在本地登录为 Administrators、管理审核和安全日志为 Administrators、修改固件环境值为 Administrators、配置单一进程为 Administrators、配置系统性能为 Administrators、从扩展域中取出计算机为 Administrators、替换进程级别标记为空、恢复备份文件和目录为 Administrators、关闭系统为 Administrators、同步目录服务数据为空、取得文件或其他对象的所有权为 Administrators。

7. 文件权限设置

目录及文件的访问原则应遵守：除非特别声明，只有 Administrators 及系统具有对系统目录及所有系统文件的完全控制，文件及目录的创建者具有对文件及其子目录的完全控制，用户的权限仅限于用户的当前目录子目录及其文件。系统管理员必须逐一检查

设置文件及目录的访问权限。

8. 注册表权限设置

除非特别需要，Administrators 或 System Full Control 对所有的键值和子键都有完全的控制权限。Creator Owner Full Control 只对子键有控制权限。Users 许可主要是对用户自身的键值、子键和值有控制权限。

15.5 本章小结

- 系统平台是指网络操作系统(network operating system，NOS)平台，即使网络上各计算机能方便而有效地共享网络资源，为网络用户提供所需的各种服务软件和有关规程的集合。目前常见的 NOS 是 Microsoft Windows NT/2000/2003/Vista 系列、UNIX 系列及 Novell 的 NetWare。
- 每个平台无论是硬件或软件，都存在着漏洞。作为网络安全的基础，网络操作系统也不例外。从某种意义上讲，系统平台的风险大小取决于网络操作系统漏洞的多少及严重程度。SANS/FBI 公布的 2006 年排名前 20 名的 Internet 最严重的安全漏洞中，网络操作系统的漏洞占了 1/3。
- 平台加固是一种用来分析及确定主机系统平台的弱点并引入适当的配置、更改及管理以保护主机及其应用程序免受攻击的方法。平台加固与网络操作系统种类密切相关。加固系统包括从系统中删除不必要的服务、软件及用户，防止系统敏感信息泄露、加强账号口令强度、使用系统审计功能及使用各种系统加固工具等措施。

习　题

1. 简述网络操作系统概念及种类。
2. 了解 Windows 及 UNIX 操作系统有哪些主要漏洞?
3. 简述系统平台加固的主要步骤。
4. 用户口令选择有哪些策略? 你了解哪些检测口令强度的工具?

第16章 应用安全

本章要点：

- 应用安全的概念及其涉及的安全服务和安全机制；
- 应用安全的风险与需求分析；
- 应用安全的体系构架；
- 应用安全的服务模式；
- 应用安全的解决方案。

16.1 应用安全概述

应用安全是指信息在应用过程中的安全，也就是信息的使用安全。按照ISO 7498-2标准给出的基于OSI七层协议参考模型的信息安全体系结构，定位于应用层的信息安全。

信息的应用涉及信息用户(即主体)和信息数据(即客体)。信息的应用过程就是主体对客体的访问和操作过程。应用安全的目的是要保证信息用户的真实性，信息数据的机密性、完整性、可用性，以及信息用户和信息数据的可审性，以对抗身份假冒、信息窃取、数据篡改、越权访问和事后否认等针对信息应用的安全威胁。

应用安全服务包括鉴别服务、机密性服务、完整性服务、访问控制服务、抗否认服务、审计跟踪服务和安全管理服务。安全服务由安全机制提供，包括鉴别机制、加密机制、完整性机制、访问控制机制、数字签名机制、抗否认机制、安全审计和报警机制、公正机制，以及可信机制、安全标记机制、事件检测机制、安全恢复机制和路由选择机制等普遍安全机制。安全服务与安全机制的关系是，一种安全服务可以通过某种安全机制单独提供，也可以通过多种安全机制联合提供；一种安全机制可以提供一种或多种安全服务。

16.2 应用安全的风险与需求

应用安全的主要风险包括身份假冒、信息窃取、数据篡改、越权访问和事后否认等。

- 身份假冒，非法用户利用合法用户的身份，访问系统资源。其风险来源主要有两点：一是应用系统的身份认证机制比较薄弱，如把用户信息(如用户名、口令)在

网上明文传输，造成用户信息泄露；二是用户自身安全意识不强，如使用简单的口令，或把口令记在计算机旁边等明处。

- 信息窃取，攻击者利用网络窃听工具窃取经由网络传输的数据包，通过分析获得重要的信息。
- 数据篡改，攻击者篡改网络上传输的数据包，使数据接收方接收到不正确的数据。数据重放也是一种对数据完整性的破坏，即攻击者抓获网络上传输的数据包，重复地发送到目的地。
- 越权访问，非法用户或者合法用户访问在其权限之外的系统资源。其风险来源于两点：一是应用系统没有正确设置访问权限，使合法用户通过正常手段就可以访问到不在权限范围之内的资源；二是应用系统中存在一些后门、隐通道、陷阱等，使非法用户（特别是系统开发人员）可以通过非法的途径进入应用系统。
- 事后否认，数据发送方或接收方抵赖曾经发送过或接收到了数据。

除了上述众所周知的风险外，还有一种容易忽视的应用安全风险，即应用系统引入安全服务和机制过程中的风险。常规的安全系统与应用系统的耦合是在应用程序中通过应用编程接口（Application Programming Interface，API）调用由专业安全厂商提供的各种安全功能模块或组件来实现，这就需要应用开发商具备一定的安全知识和技能，才能将这些不同的安全功能模块有机地结合，实现应用系统所需的安全特性和级别。但是，普遍的应用开发商毕竟不是专业安全厂商，加之安全问题比应用问题更加复杂，因此，上述耦合方式不仅增加了应用系统的复杂度和应用开发商的负担，而且在耦合过程中容易出现新的安全漏洞，不能保证最终系统达到预想的安全水准。所以，在安全体系设计时，要充分考虑“应用安全实现的可控性”，以便尽可能地降低安全系统与应用系统结合过程的风险。

应用安全需求包括两个方面：一是应用安全服务和机制，即面向应用的安全系统自身；二是安全系统与应用系统的结合。应用安全服务和机制可参见第 4 章。

安全系统与应用系统的结合是实现应用安全的必要过程，这一过程是存在风险的。两者结合的效果直接影响着最终的系统安全水准，有必要采取有效方法和措施保证两者的低风险结合。为了把两者的结合过程对安全水准的影响降到最低点，保证结合后的系统达到安全系统提供的最高安全水准，需要把握如下几点原则：

- 保持安全系统与应用系统的相互独立性，避免功能实现上的交叉或跨越。
- 避免程序级别的低层接口，免除两者结合时应用系统的二次编程开发。
- 增强安全系统的适用性，最大限度地提供便捷可靠的结合方式。

16.3　应用安全的体系结构

应用安全服务是建立在能够提供信任服务的基础设施之上的。这一点与各种电器设备建立在电力基础设施上的道理是一样的。只有在公认和权威的信任设施之上，各种应用安全服务才能有可靠的根基，才能提供可信的服务。

公钥基础设施（Public Key Infrastructure，PKI）作为国际上公认和普遍采用的信

息安全保障体系的基础设施，提供信任和安全服务。PKI 利用公钥理论和技术建设具有通用性的、高水准的安全基础设施，目标是全面提高建立在其上的应用系统的安全水平。

影响 PKI 推广的因素分析如下：

- 正面因素，Internet 的普及和应用，特别是电子商务和电子政务等高安全级别的应用，对无用户边界的 Internet 的信任机制提出了严格要求，PKI 也因此应运而生。PKI 中的可信第三方——证书认证中心（Certificate Authority，CA），可以解决无边界用户的身份确定问题，提供了信任的基础。因此，当今网络应用，特别是基于 Internet 的应用需要 PKI。
- 负面因素，PKI 自身机制具有一定的复杂度，除了 CA 的建设、维护和管理，使用好 CA 颁发的数字证书也不是一件轻松的事情，需要一定的安全知识、技能和编程工作。因此，还不能像电力基础设施，只要插上电源插座便可使用那样，容易推广使用。
- 可控因素，如何使 CA 与应用能够安全和便捷地相结合是一个可控制的因素，做得好便成为促进 PKI 推广的正面因素，做不好便成为阻碍 PKI 推广的负面因素。

全面的 PKI 理解应包括两个方面：一个是数字证书的签发和管理，另一个是数字证书的使用。

证书认证中心是数字证书的签发和管理机构，证书反映持有者的身份。如同国家护照管理部门与护照、信用卡公司与信用卡的关系，CA 从功能和服务上讲，只负责证书的签发和管理，证明证书与持有者的关系。同时提供诸如加解密、数字签名等与证书相关的安全功能模块。但如何使用证书及其相关的安全功能模块满足应用系统的实际安全需求，不是 CA 的任务。

应用安全中心（AAs）负责数字证书的使用，实现面向应用的各种安全服务，以满足各种环境下不同应用的安全需求。AAs 表示以身份认证中心 AA（Authentication Authority）、授权中心 AA（Authorization Authority）、审计中心 AA（Audit Authority）和管理中心 AA（Administration Authority）等为代表的应用安全机制中心。AAs 为应用系统提供整套且有机结合的安全服务，起着 CA 通向应用的桥梁和纽带作用。

综上所述，CA 是应用安全服务的信任基础，AAs 是应用安全服务的具体实现，CA＋AAs 应用是对 PKI 的全面理解（详见表 16-1）。CA、AAs 和应用的关系如图 16-1 所示，即 CA 是核心和基础，AAs 是桥梁和纽带，应用是目标。

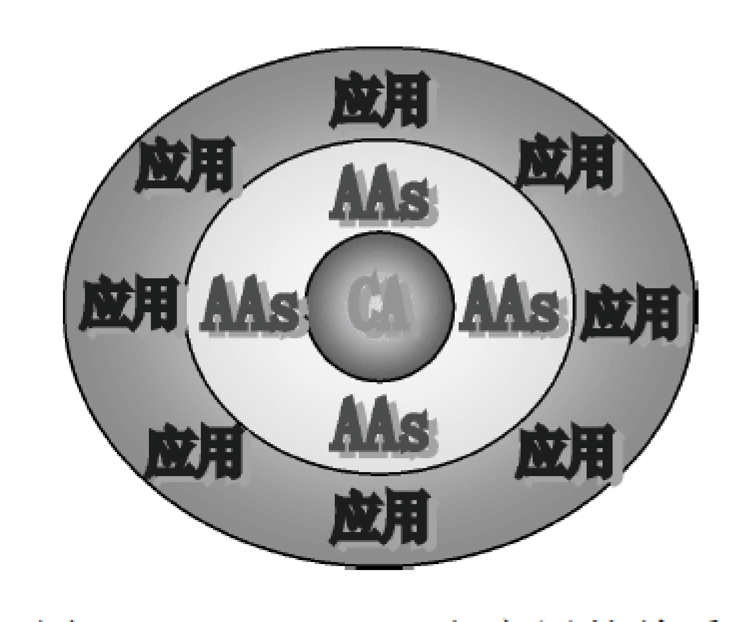


图 16-1　CA、AAs 和应用的关系

表 16-1　证书认证中心(CA)+应用安全中心(AAs)

安全构架	安全功能	安全机制	
		名　称	内　容
CA+AAs	证书的签发和管理	证书认证中心(CA)	证书认证中心(Certificate Authority)
	证书的使用	应用安全中心(AAs)	身份认证中心(Authentication Authority)、授权中心(Authorization Authority)、审计中心(Audit Authority)、管理中心(Administration Authority)等面向应用的其他安全机制中心

16.4 应用安全的服务模式

应用安全中心为应用系统提供安全服务，其服务模式有两种：

- 纵向安全服务模式；
- 横向安全服务模式。

16.4.1 纵向安全服务模式

纵向安全服务模式(见图 16-2)的特点是，安全系统介于应用系统与操作系统之间，即纵向切入，以 API 程序接口的形式提供安全功能，应用系统使用 API 调用安全系统提供的安全模块，来实现其安全目标。因此，应用系统为引入安全特性，不可避免地要进行二次编程开发。

应用系统
API
安全系统
API
操作系统

图 16-2　纵向安全服务模式

纵向安全服务模式采用的系统结构如图 16-3 所示。各应用系统的服务器和客户端均在程序级与安全系统结合，即应用程序通过 API 调用安全模块。

纵向安全服务模式是一种分散的实现方式，容易导致重复和低水平的开发。也是一种被动的结合方式，安全系统提供的安全功能模块要靠应用系统去修改程序进行调用才能发挥作用。

综合上述分析，纵向安全服务模式存在的问题归纳如下：

- 实现的可控性问题。一般应用开发方不是专业安全厂商，缺乏足够的安全知识和技能，加之安全问题的复杂性，虽然有现成的安全功能模块，但也不能完全保证它们使用好这些安全功能模块，真正达到保护应用信息的目的。一旦应用系统中某个应用出现安全漏洞，那么整个应用系统的安全水准会降到这个最低点，这就是所谓的安全体系的“木桶”效应。

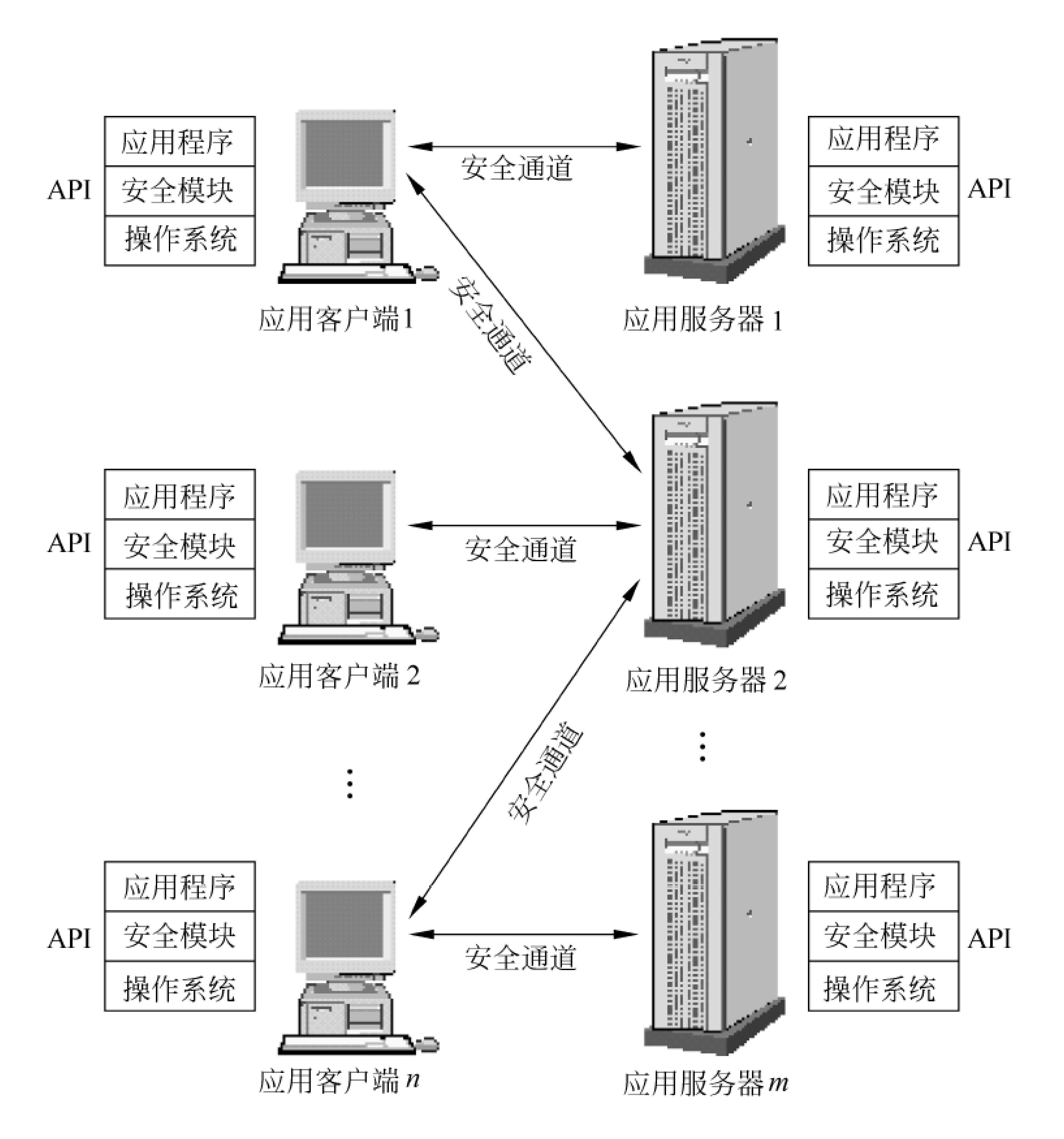


图 16-3　纵向安全服务模式的系统结构

- 系统的可维护性问题。新的安全威胁不断出现，安全系统需要相应地不断升级。因此，安全系统是动态的，不是一成不变的。由此导致的安全功能模块或其 API 的变更，会引起应用系统与安全相关各部分的重新安装、重新编译，甚至重新编写，给应用系统安全性的维护造成极大的困难，甚至混乱。在这种情况下，就更难避免安全漏洞的出现。

16.4.2　横向安全服务模式

横向安全服务模式（见图 16-4）的特点是，安全系统介于应用客户端和应用服务器之间，即横向切入，以安全过滤器的形式为应用系统提供安全服务，无 API 程序级接口，也就无需应用系统为此进行再次编程开发，只需对安全过滤器按照应用的安全策略进行安装和配置即可。

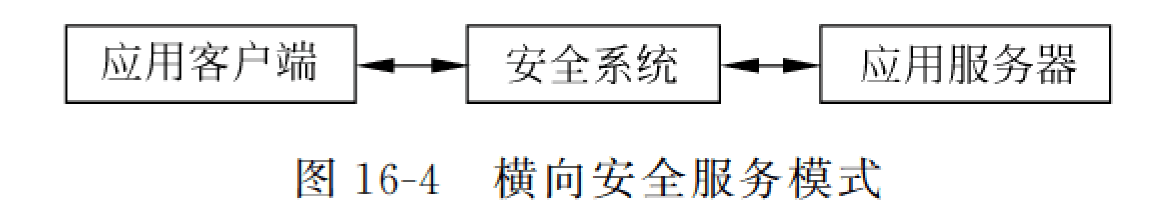


图 16-4　横向安全服务模式

横向安全服务模式采用的系统结构如图 16-5 所示。与纵向安全服务模式不同，各应用系统不在程序级与安全系统结合，因此应用系统的服务器程序和客户端程序均不需要

修改。

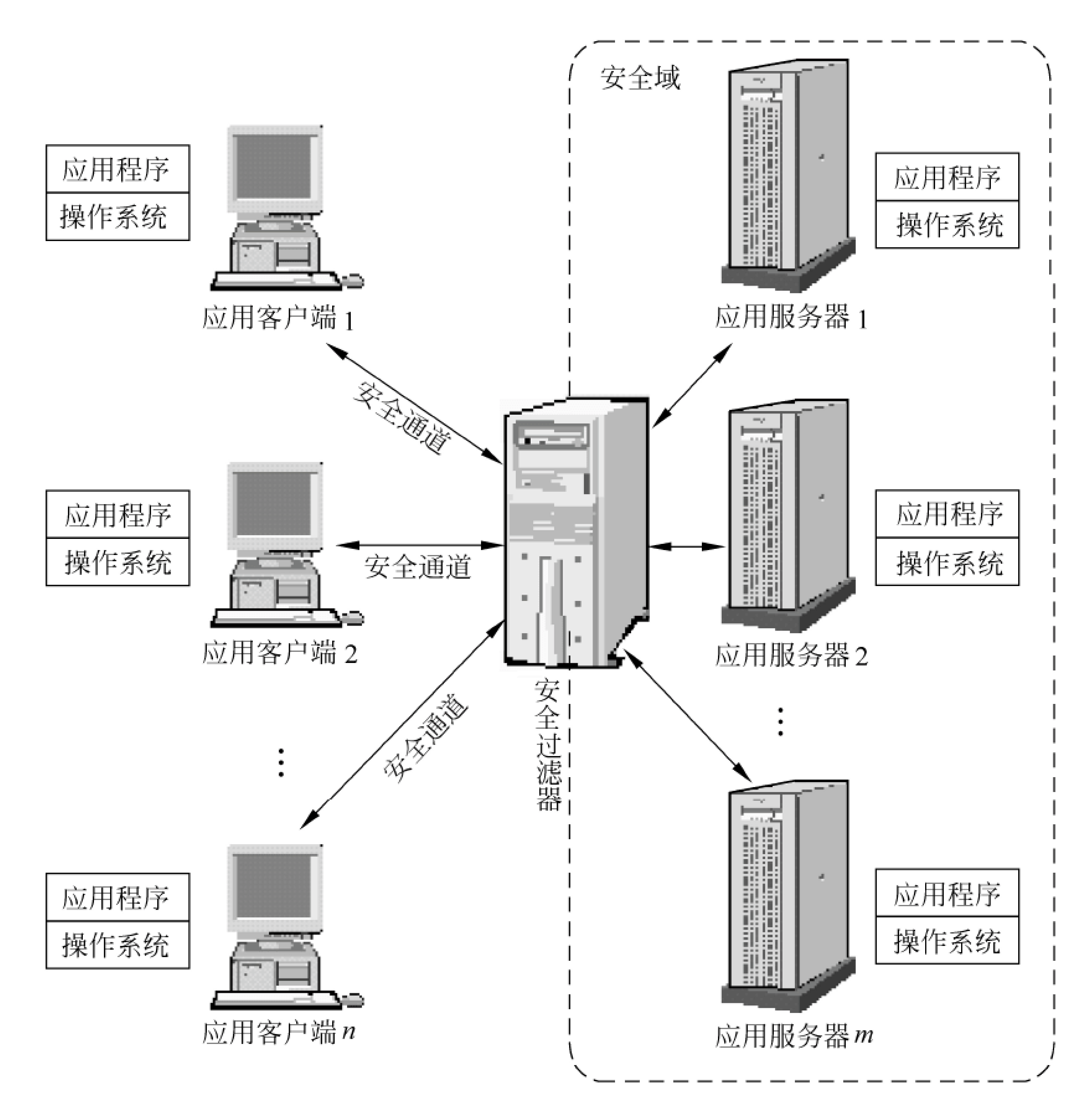


图 16-5　横向安全服务模式的系统结构

横向安全服务模式是一种集中的实现方式，可避免重复和低水平的开发。也是一种主动的结合方式，只需配置安全系统，不需修改应用系统程序，便能提供安全服务。

横向安全服务模式的基本工作原理为：通过客户端配置或客户端安全代理，应用客户端的请求不是直接送往应用服务器，而是送到安全过滤器，经过安全过滤器依据事先设置的安全控制策略进行过滤并通过之后，才能送往应用服务器，否则拒绝应用请求。

横向安全服务模式中的安全过滤器提供如下功能和服务：

- 安全通道。应用客户端与安全过滤器之间的通道是经过双方的加密通道，保证它们之间通信的安全性。
- 安全域。为需要保护的资源(应用服务器及其上的信息资源)提供安全空间，可通过系统和网络的配置将被保护的资源纳入安全空间。在进行系统和网络配置时，必须保证应用客户端的请求只能经过安全过滤器才能进入安全域，在物理网络上不能有旁路或后门。
- 集中管理。可将用户、资源以及用户对资源的访问权限在逻辑上统一管理，实施统一的安全策略。
- 分布控制。可将安全功能的实现机制分散部署，实施分布式的安全控制，提高安

全系统的可用性和可靠性，防止性能瓶颈和单点失效。

横向安全服务模式的优越性体现在如下方面：

- 获得高性能价格比。横向安全服务模式提供的全套和高质量的安全功能，既可以免去应用开发方重复开发各自的安全功能，又可以得到高水平的和不断升级的安全功能。高水平的安全功能的开发难度通常高于应用功能本身。根据统计，高安全需求的应用系统如果自行开发安全功能，其开发量平均占总开发量的二分之一以上。使用横向安全服务模式将极大地简化有安全需求的应用系统的开发，提高开发效率，降低开发和维护成本，同时保证安全功能的高质量。
- 实施统一安全策略。横向安全服务模式提供的集中管理和分布控制功能，可以实施统一的安全策略，避免安全孤岛和安全弱点的出现，从而保证系统整体的安全水准。安全孤岛出现是因为应用系统自行开发独自的、非标准的安全功能，不能与其他应用系统进行互操作，导致应用系统之间的交互安全没有保证，因此全局的安全也无法保证。安全弱点出现是因为应用系统自行开发的安全功能很难达到高水准的安全级别，容易产生安全的薄弱环节。按照“木桶”效应（木桶中的水准与最低木板的高度相等），系统整体的安全水准等于最薄弱环节的安全水准。采取集中管理和实施统一安全策略是解决安全孤岛和安全弱点的有效途径。
- 可持续发展。横向安全服务模式的安全系统独立于应用系统，便于应对新的安全需求，开发新的或增强的安全功能，从而保证安全体系的可持续发展。安全系统升级换代后，运行其上的应用系统的安全功能也随之自动升级换代。

总之，在实现方式、结合方式和安全保证等各方面，横向安全服务模式明显优于纵向安全服务模式。

16.5　网络应用安全平台

WebST 是一款实现应用安全中心（AAs）的典型产品。以下从 WebST 的服务模式、系统结构、工作流程、系统部署、安全管理方面进行较全面介绍。

16.5.1　WebST 的服务模式

WebST 采用横向安全服务模式（图 16-6），克服了纵向安全服务模式的弊端。有关横向安全服务模式的概念、特点和优势已在前面论述了，这里不再重复。

WebST 安全服务器系统作为安全过滤器，包括安全认证服务器、安全控制服务器和安全管理服务器，提供面向应用的整套安全服务。WebST 安全客户端截获应用客户端访问安全域中应用服务器上被保护资源的请求，经由安全通道提交给 WebST 安全服务系统进行安全过滤，即身份认证和访问控制，决定该请求是否允许通过。如果通过了身份认证和访问控制的审查，则将该请求传递给安全域中相应的应用服务器，并将应用服务器的处理结果返回给应用客户端；否则拒绝该请求进入安全域，并给应用客户端返回相应的安全错误信息。

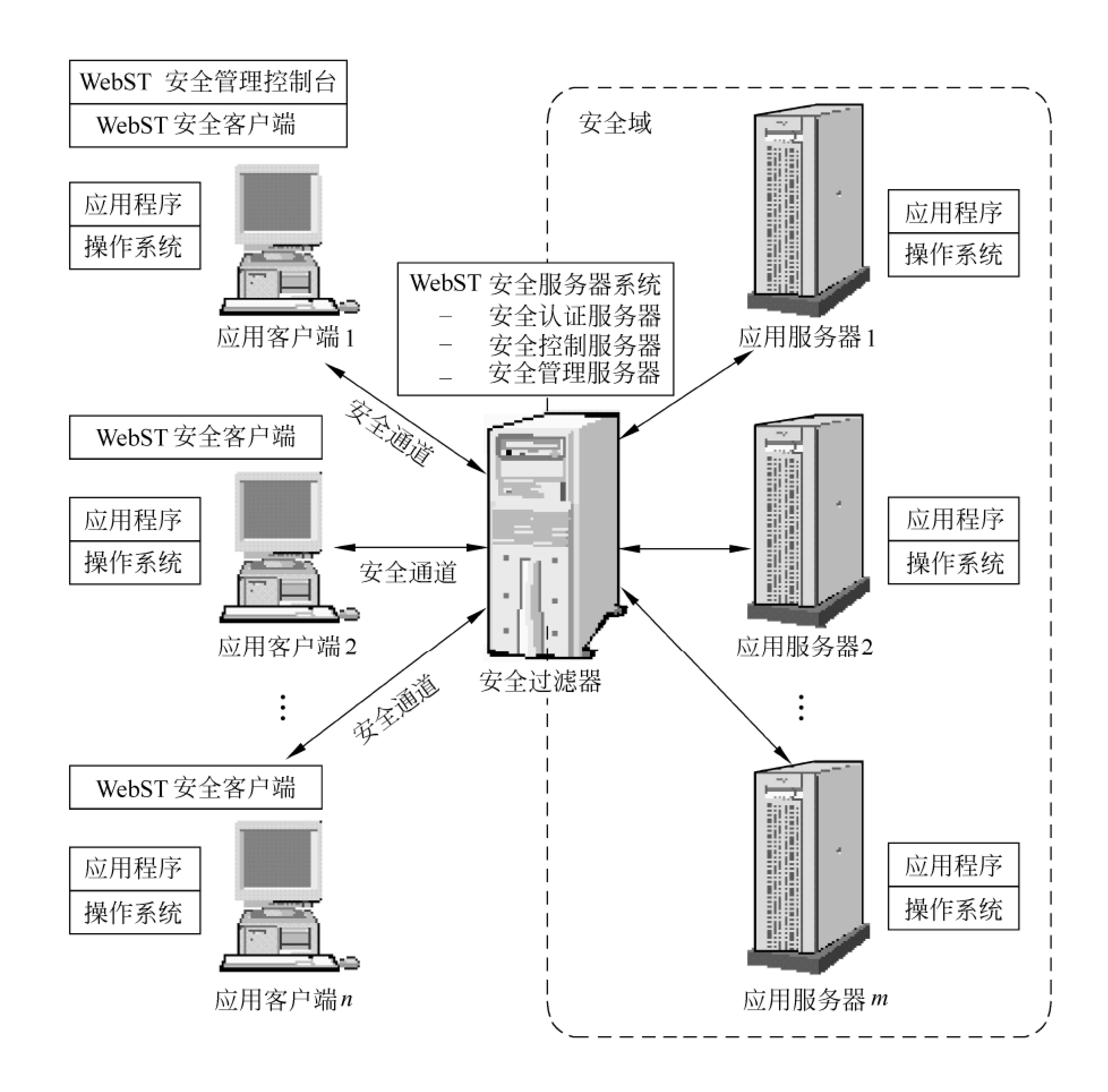


图 16-6　WebST 的横向安全服务模式

16.5.2　WebST 的系统结构

WebST 的系统结构如图 16-7 所示。该系统由安全认证服务器、安全控制服务器、安全管理服务器、安全管理控制台和安全客户端，以及用户注册数据库和授权策略数据库组成。

WebST 各组件的功能和关系如下：

- 安全认证服务器凭借用户的身份信息（用户名/口令或数字证书）和安全服务器的身份信息（注册信息或数字证书），查询用户注册数据库，完成双向身份认证，并为通过认证的用户发放一个用户凭证；
- 安全控制服务器依据用户凭证，查询授权策略数据库，获得用户对所需资源的访问权限，进而决定是否允许用户访问所需资源；
- 安全管理服务器和安全管理控制台为管理员提供注册新来用户、配置新增资源和设置访问权限的服务和操作界面；
- 安全客户端截获用户请求，与安全控制服务器建立安全通道，将用户信息和用户请求通过安全通道传给相应的安全控制服务器；

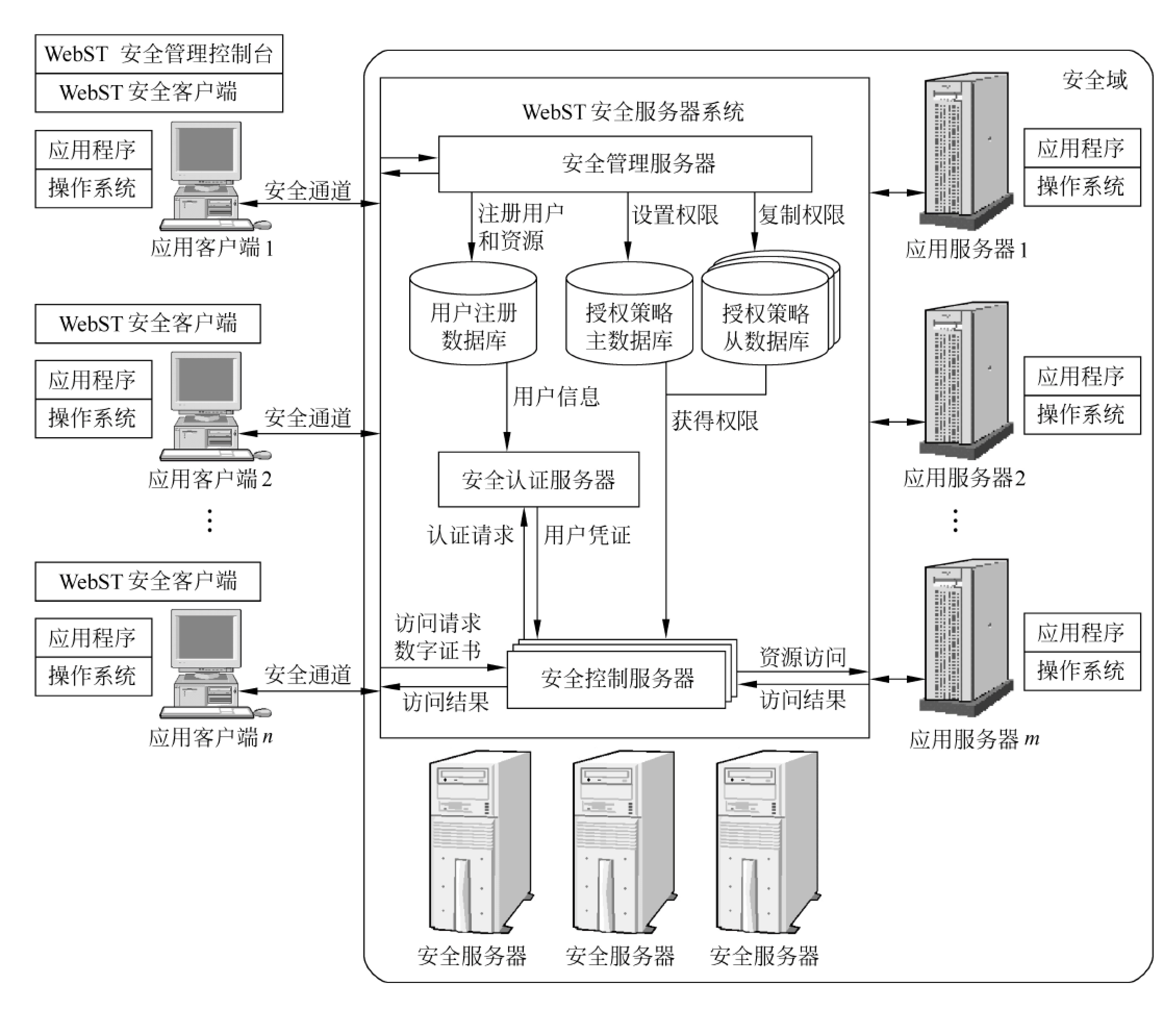


图 16-7　WebST 的系统结构

- 用户注册数据库存储注册用户的各种属性信息和被保护资源的位置信息；
- 授权策略数据库存储用户对资源的访问权限信息。

WebST 具有逻辑上的集中管理和物理上的分布控制特性。可以有多个安全控制服务器和复制的授权策略从数据库在网络中分散到需要的地方，即可提高性能，也可增加容错性。

WebST 中的各安全服务器之间以及与应用客户端的通信都是经过加密的安全通道。

16.5.3　WebST 的工作流程

1. 系统配置

系统管理员利用安全管理控制台，通过安全管理服务器在用户注册数据库中建立用户账号和资源目录，并根据应用的安全管理策略设置注册用户对被保护资源的访问权限。

2 身份认证

当用户通过应用客户端访问应用系统，输入访问请求时，安装在应用客户端上的安全客户端软件捕获该请求，然后与安全控制服务器和安全认证服务器建立安全通道，利用安

全通道完成身份认证的过程。首先要求用户提供必要的用户身份信息(如用户注册名/口令或数字证书),然后采用 Kerberos v5(对称密钥技术)或 PKI(非对称密钥技术)身份认证机制完成认证,并给通过认证的用户返回一个用户凭证。该认证过程既支持用户对服务器的身份认证,也支持服务器对用户的身份认证,即支持双向身份认证。

3. 访问控制

身份认证通过后,安全控制服务器得到来自安全认证服务器的用户凭证和来自安全客户端的访问请求。安全控制服务器查看授权策略数据库,决定用户是否具有对所请求资源的访问权限。如果有,则把该访问请求提交给后面安全域中的应用服务器,得到访问结果后,再通过安全通道返回给应用客户端。

4. 安全审计

上述系统管理员和用户的操作全过程均以日志文件的形式记录在案。

16.5.4　WebST 的系统部署

WebST 可以在物理上分散和复制部署,以适应不同规模的应用环境,同时,既可加强可靠性,也可提高可用性。

图 16-8 给出了安全控制服务器和授权策略数据库的分散和复制部署。多个安全控制服务器分散部署在不同的地方,保护当地的应用服务器。所有远离授权策略主数据库的安全控制服务器都带有由授权策略主数据库复制而来的授权策略从数据库。因此,安全控制服务器在进行访问控制时,只需要查询本地的授权策略数据库即可。

安全客户端根据用户请求访问的资源地址(如 URL),判断所要访问资源所在的应用服务器,将用户的访问请求提交给保护该应用服务器的安全控制服务器。

安全认证服务器也可以进行与安全控制服务器类似的分布式部署。

16.5.5　WebST 的安全管理

WebST 提供统一管理界面、统一用户注册、统一资源目录、统一授权策略、用户分组管理、用户分级管理和系统设置等安全管理功能。

1. 统一管理界面

WebST 集用户管理、资源管理和安全策略管理于一体,为管理者提供统一的操作界面(见图 16-9)。

2. 统一用户注册

WebST 允许建立一个统一的组织机构树,在组织机构树的背景下创建和维护用户(见图 16-10)。用户分为管理员和普通用户两种(见图 16-11)。

3. 统一资源目录

WebST 通过其独有的灵巧连接技术提供一个统一的名字空间,也就是安全域的资源名字空间。在 WebST 安全管理服务器上,可以通过配置,将需要保护的资源,在这一名字空间中集中命名(见图 16-12)。

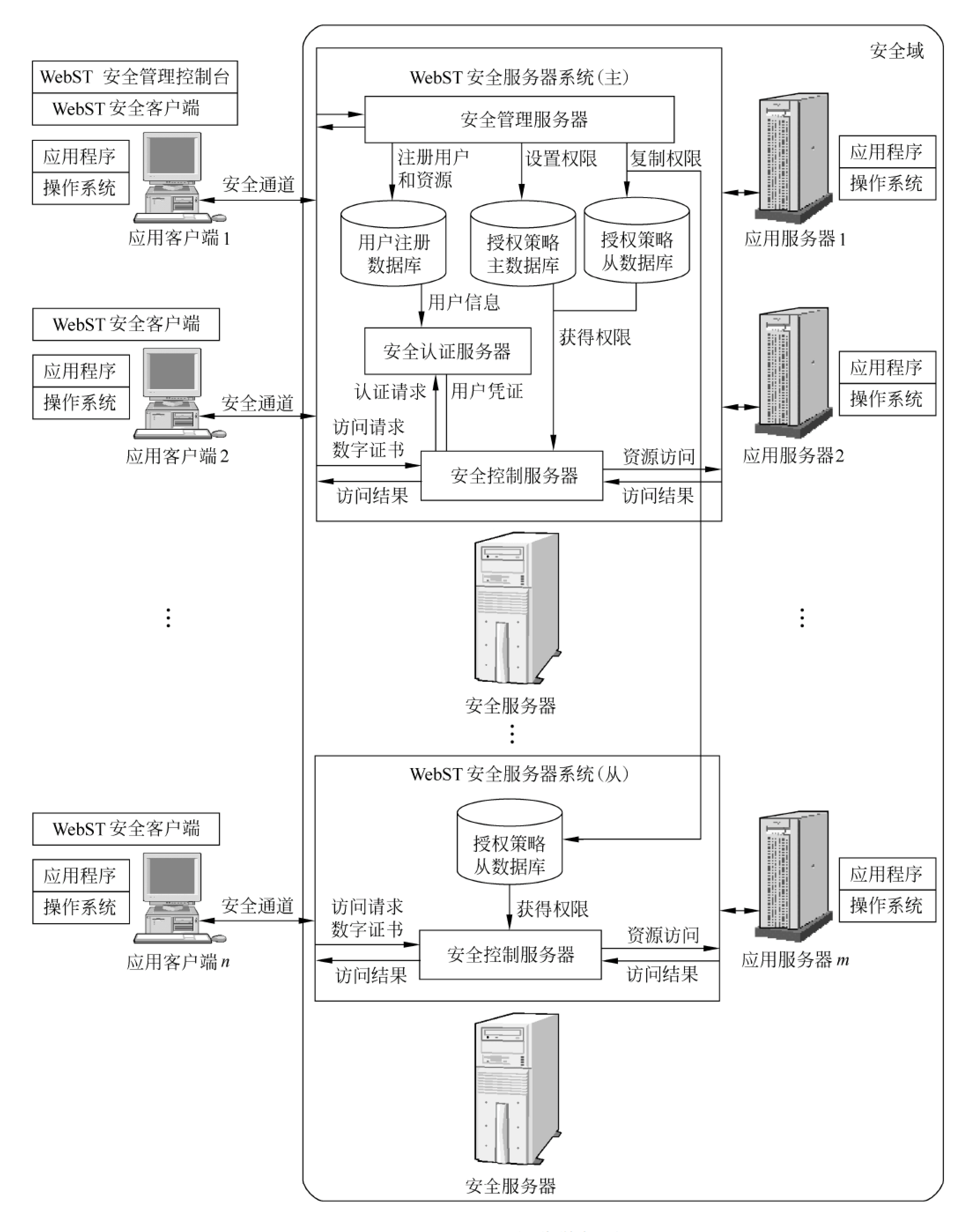


图 16-8　WebST 的分散部署

4. 统一授权策略

WebST 的用户和资源的集中管理，为实施统一访问授权提供了可能。WebST 设置访问权限的方法为，首先创建基于角色的授权策略模板(见图 16-13)，然后将授权策略模板应用到资源目录树上的结点，即加锁的位置(见图 16-14)。授权策略模板可以共享和修改。

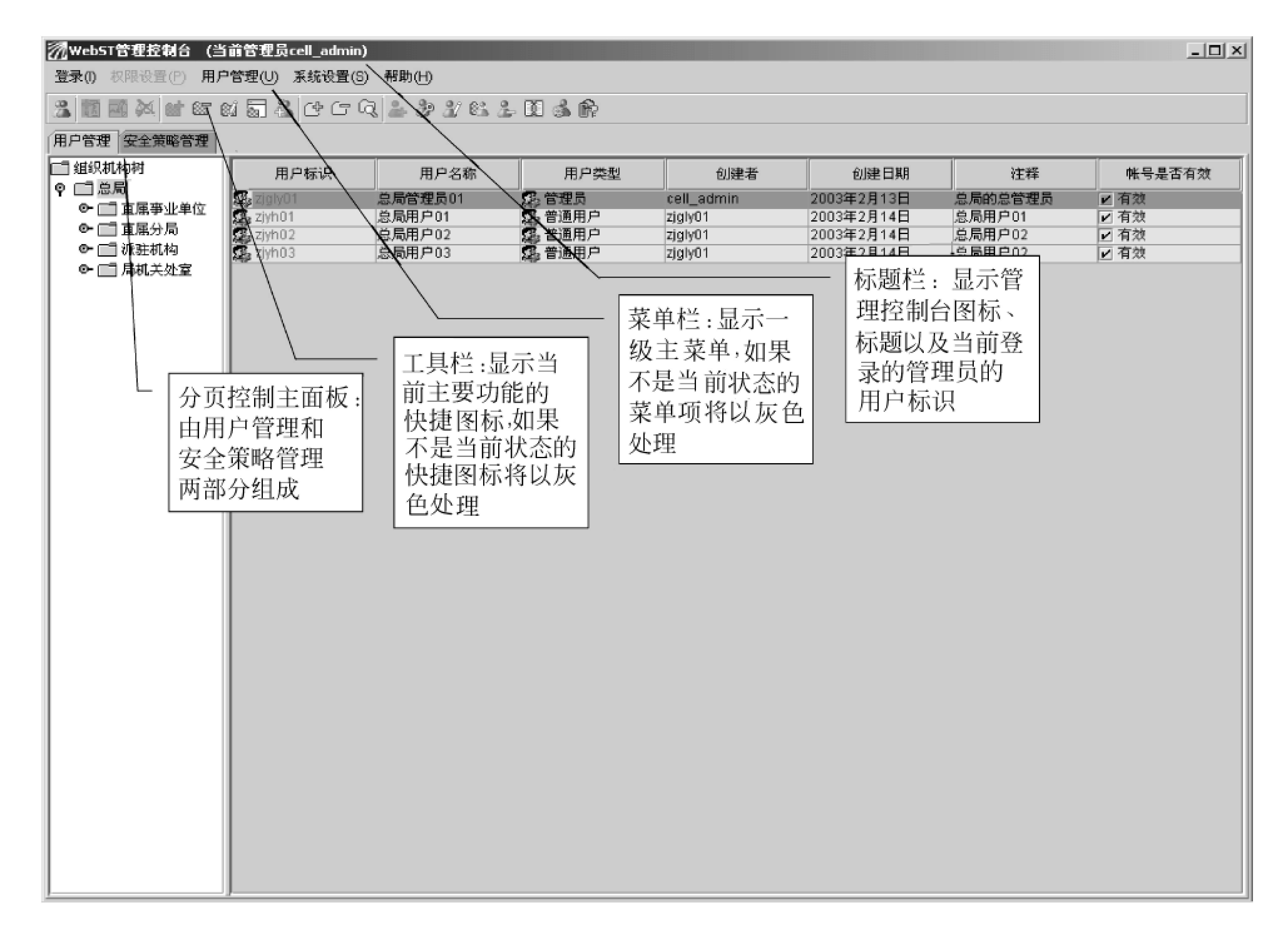


图 16-9　WebST 管理控制台

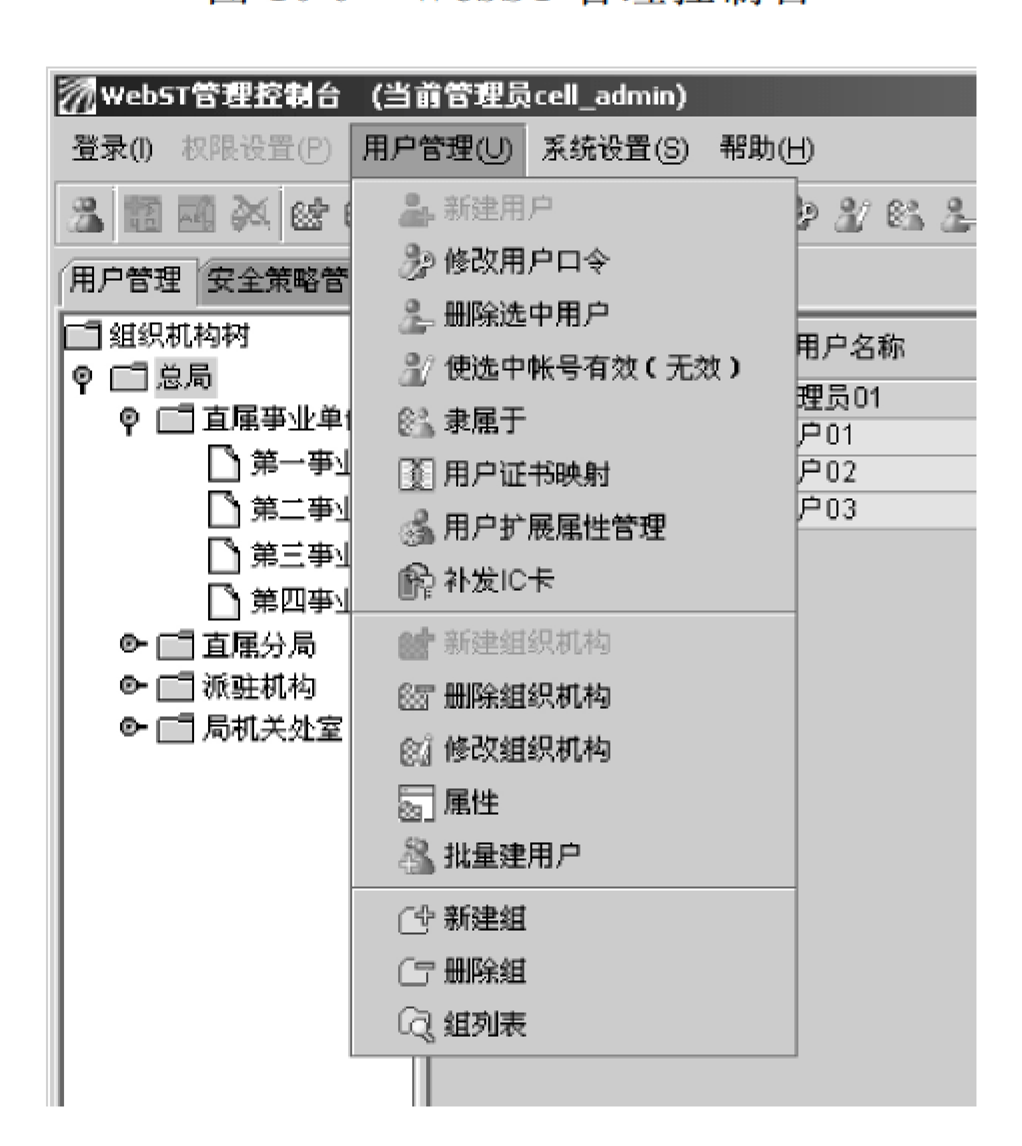


图 16-10　WebST 的用户管理

用户标识	用户名称	用户类型	创建者	创建日期	注释	帐号是否有效
zjgly01	总局管理员01	管理员	cell_admin	2003年2月13日	总局的总管理员	☑ 有效
zjyh01	总局用户01	普通用户	zjgly01	2003年2月14日	总局用户01	☑ 有效
zjyh02	总局用户02	普通用户	zjgly01	2003年2月14日	总局用户02	☑ 有效
zjyh03	总局用户03	普通用户	zjgly01	2003年2月14日	总局用户03	☑ 有效

图 16-11　WebST 的用户类型

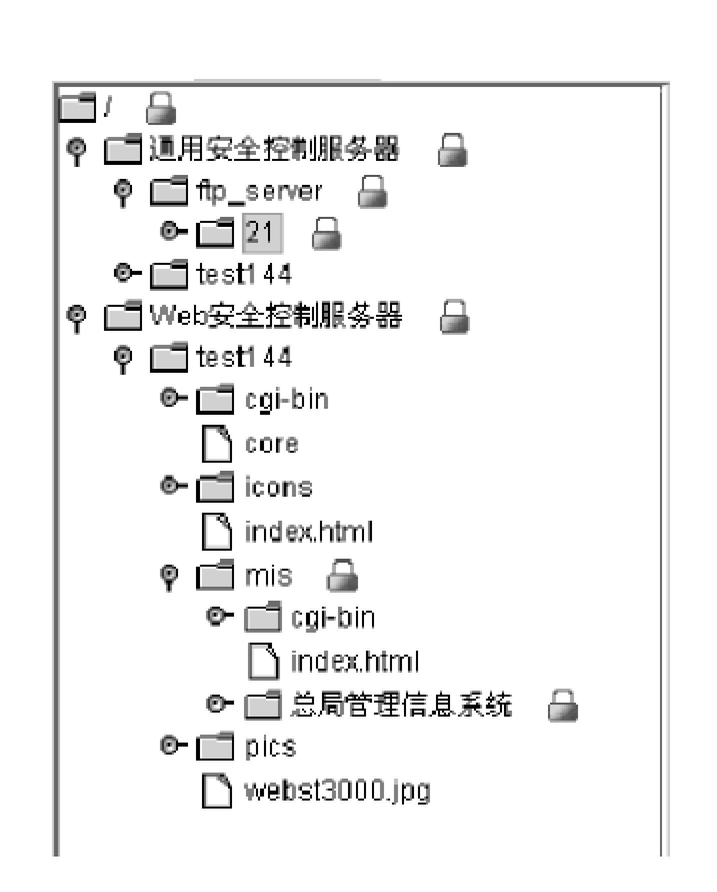


图 16-12　WebST 的资源目录



图 16-13　WebST 创建授权策略模板

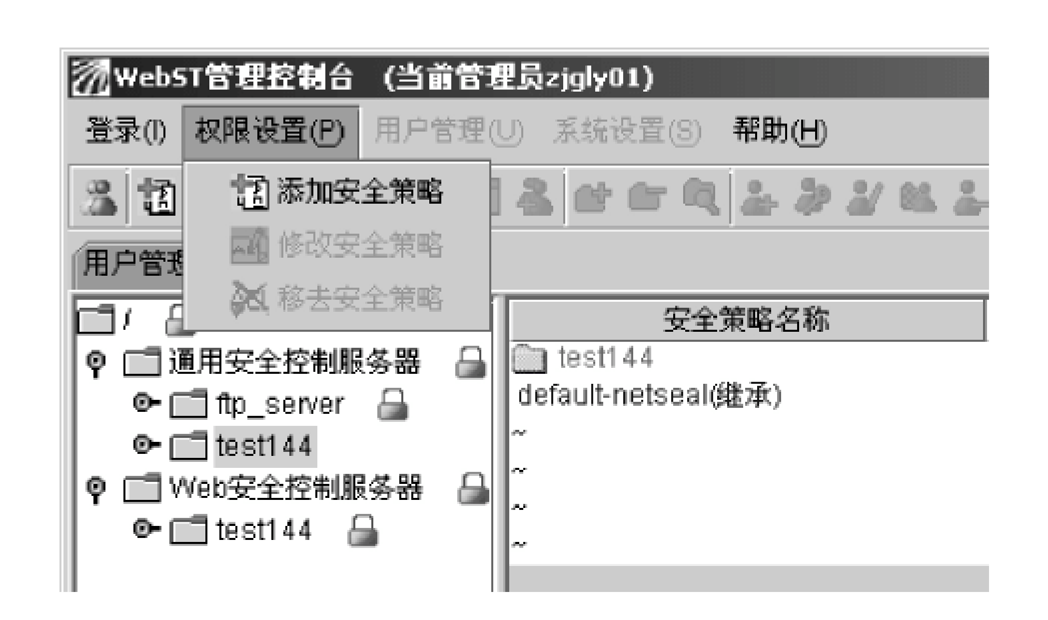


图 16-14　WebST 应用授权策略模板



图 16-15　WebST 的用户分组管理

5. 用户分组管理

针对用户访问资源，WebST 提供分组管理，即允许将具有相同访问权限或扮演同样角色的用户分在同一组内（见图 16-15）。因此，通过对组进行权限设置，就达到了对组内所有用户的权限设置。

6. 用户分级管理

针对管理员管理用户，WebST 提供分级管理，即上级管理员将其管辖的部分用户全权委托给下级管理员代理管理。其效果是，上级管理员可以看到下级管理员管理的用户信息，但无权进行增、删、改操作；而下级管理员只能访问到其管辖范围的用户，无法看到其上级管理员的用户信息（见图 16-16）。

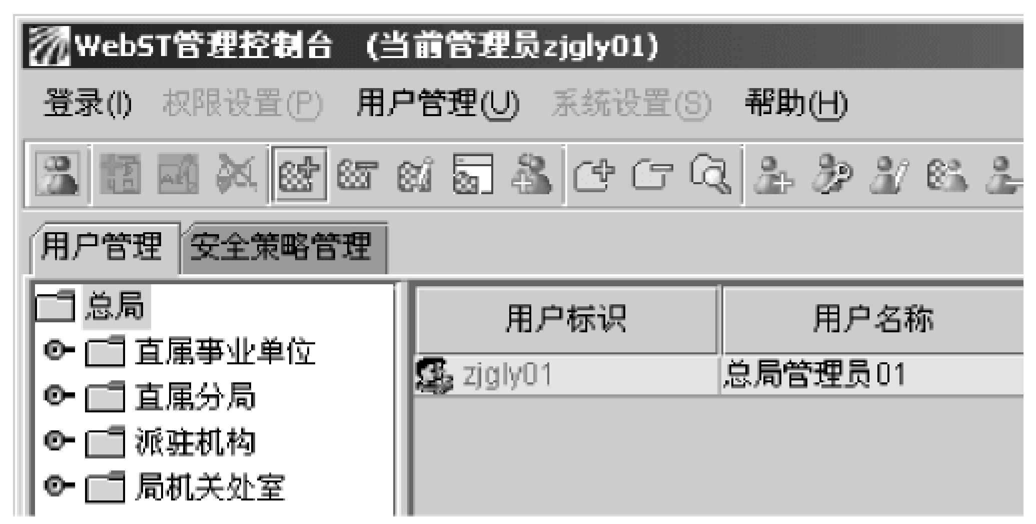




图 16-16　WebST 的用户分级管理

16.6　本章小结

应用安全是指信息在应用过程中的安全，也就是信息的使用安全。应用安全的目的是要保证信息用户的真实性，信息数据的机密性、完整性、可用性，以及信息用户和信息数据的可审性，以对抗身份假冒、信息窃取、数据篡改、越权访问和事后否认等针对信息应用的安全威胁。

安全系统与应用系统的结合是实现应用安全的必要过程，这一过程是存在风险的。两者结合的效果直接影响着最终的系统安全水准，有必要采取有效的方法和措施保证两者的低风险结合。

应用安全服务是建立在能够提供信任服务的基础设施之上的。公钥基础设施 PKI 作为国际上公认和普遍采用的信息安全保障体系的基础设施，提供信任和安全服务。对 PKI 的全面理解应是证书认证中心（CA）＋应用安全中心（AAs）。即 CA 是核心和基础，AAs 是桥梁和纽带，应用是目标。

应用安全中心为应用系统提供安全服务，其服务模式有两种：纵向安全服务模式和横向安全服务模式。在实现方式、结合方式和安全保证等各方面，横向安全服务模式明显优于纵向安全服务模式。

网络应用安全平台 WebST 是一款实现应用安全中心的典型产品，具有优越的横向

安全服务模式、统一的资源命名、分布式的系统部署、整套安全功能的有机结合、多样的身份认证机制、安全的分级管理等特色，并在多年的实际应用中得到了实践的验证，证明是一款有效的应用安全解决方案。

习 题

1. 阐述应用安全的概念和内容。
2. 应用安全需求包括哪两方面？
3. 阐述应用安全的体系构架以及 CA、AAs 和应用的关系。
4. 阐述横向安全服务模式和纵向安全服务模式的区别和利弊。
5. 网络应用安全平台 WebST 是(　)的实现。

   A. CA　　　B. AAs　　　C. 应用

第 4 篇
网络安全工程

第17章 安全需求分析

本章要点:
- 安全需求的范围和目标;
- 安全威胁的数据分析;
- 管理安全的关键、范围和需求以及安全模型的核心组成;
- 运行安全的范围和需求;
- 技术安全的范围和需求;
- 基于信息等级分类策略的基本安全属性需求;
- 基于信息等级分类策略的用户标识与鉴别需求;
- 基于信息等级分类策略的不可否认需求;
- 基于信息等级分类策略的授权与访问控制需求;
- 网络基础设施安全需求。

网络安全需求是根据安全策略导出的,在第3章已经阐明了各种网络安全策略。合适的安全需求可以较小的代价控制风险,包括管理、运行、技术控制3方面的需求,以满足信息资产的机密性、完整性、可用性和可审性。本章将定义基于互相联系的管理、运行、技术控制的网络信息安全需求。

可以将需求定义成一个系统必须遵守的条件或能力。这里指的系统包括商业经营、事务处理、操作系统、应用程序、数据库平台、网络组件和系统有关的经营单元与责任以及涉及个人的处理过程等。

网络安全的主要目的是保护一个组织的信息资产的机密性、完整性、可用性。确定和管理网络信息安全需求对一个组织减少风险是至关重要的。这里讲述的是网络安全的基本需求,并以大企业网络安全需求为例,由于各个组织的情况很不一样,因此在实际工作中,各个组织还应确定反映本组织实际情况的网络安全需求。在以下的阐述中用了“必须”和“应该”两个不同的词,前者表示必须遵循的、对安全要求高的系统则是强制性的,后者表示对一般系统希望能达到。

在定义网络安全需求之前,首先阐述对安全的各种威胁,这是基于第2章风险分析基础上的一些数据分析。

17.1 安全威胁

当今的企业经营环境,愈来愈多地使用Internet和分布计算,为客户提供各种服务以及帮助员工提高工作效率。随着更多的信息共享、Internet的广泛使用、电子商务基础设

施的部署，企业面临的漏洞和威胁也愈益增加，如内联网（Intranet）、外联网（Extranet）、供应链网的漏洞和威胁。

这些威胁有可能损害企业的人力资源和网络资源。威胁可能来自外部黑客非授权使用系统的漏洞，也可能来自内部员工做一些非业务的活动。其结果是内部信息的泄露、客户记录和秘密的经营信息数据的破坏、产品的损伤等。

根据美国计算机安全研究所（CSI）和联邦调查局（FBI）所做的“2000 年计算机犯罪和安全调查”，有 90% 的被调查对象（273 个组织）在 2000 年受到攻击，经济损失为 265 589 940 美元，比 1997、1998、1999 前 3 年的统计要高很多，前三年的年平均经济损失为120 240 170 美元。根据分析，大部分严重的经济损失是由于内部信息的偷窃，如图 17-1 所示。

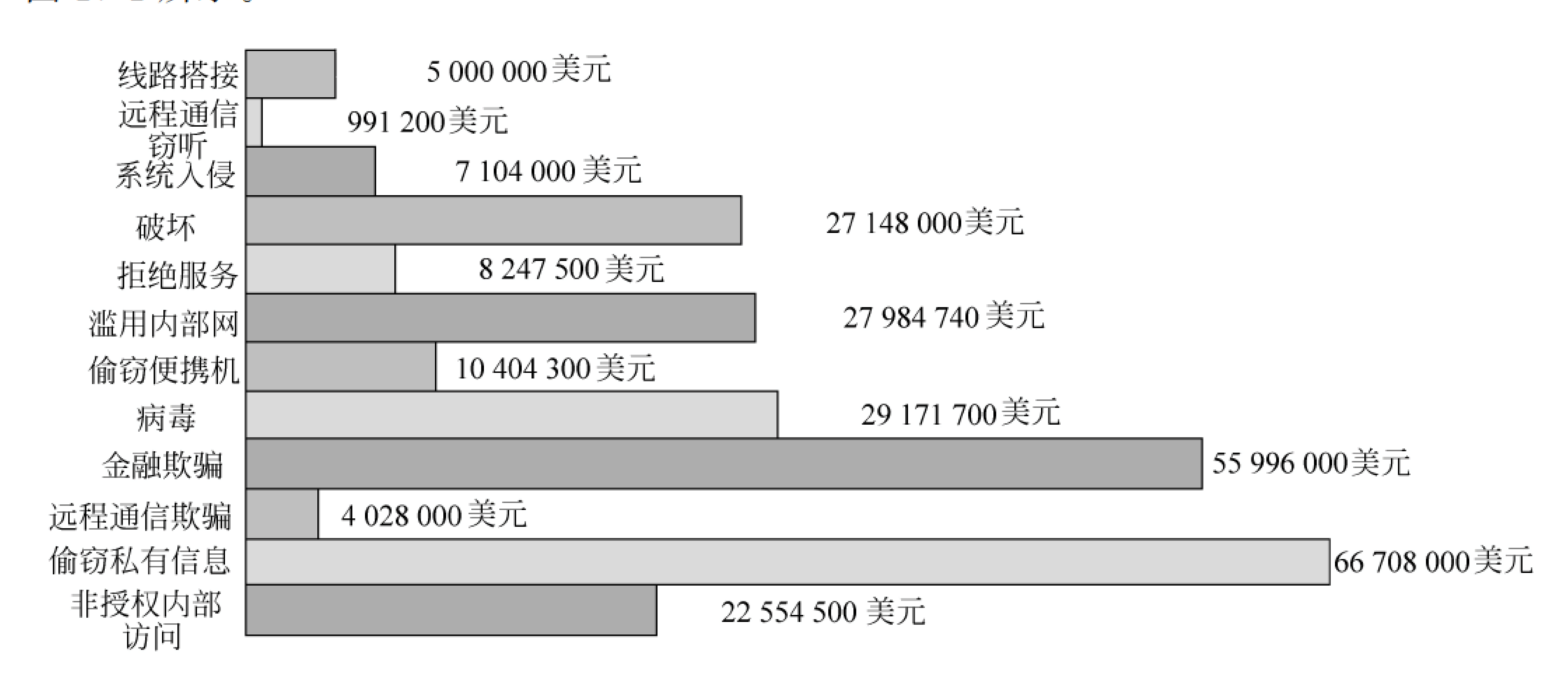


图 17-1　攻击和滥用造成的经济损失

数据来源：美国 CSI/FBI 2000 年计算机犯罪和安全调查

由威胁引起的损失可分成直接损失和间接损失两类。直接损失是指一个系统或其相关的组件受损；间接损失是指由于直接损失引起的后果。这些后果包括丢失客户、丢失供应者、丢失公共的信誉、丢失竞争的优点和信息、丢失有形资产和减少现金流等。间接损失通常占总损失的大部分，可达 90%～95%，成为安全重点保护的方面。

在不断变化的数字经济时代，威胁来自各种各样的源，也可分成各种类型。这里将威胁分成两大类，即外部威胁和内部威胁。

17.1.1　外部安全威胁

常见的外部安全威胁是黑客破坏企业的 Web 站点，涂改 Web 页面，而且这种破坏的趋势日益增多，图 17-2 是某公司在 1999～2000 年遭受的 Web 损毁和涂改的次数。

随着 Internet 的广泛使用，并成为企业日常运行不可缺少的工具和环境，传统的物理世界的偷窃和诈骗迁移到网络世界。除了涂改 Web 页面外，通过 Internet 发出的攻击还有伪装成其他用户、分组回答、拒绝服务、字典攻击、系统标识假冒、通信窃听、特洛伊木马、病毒和蠕虫等。

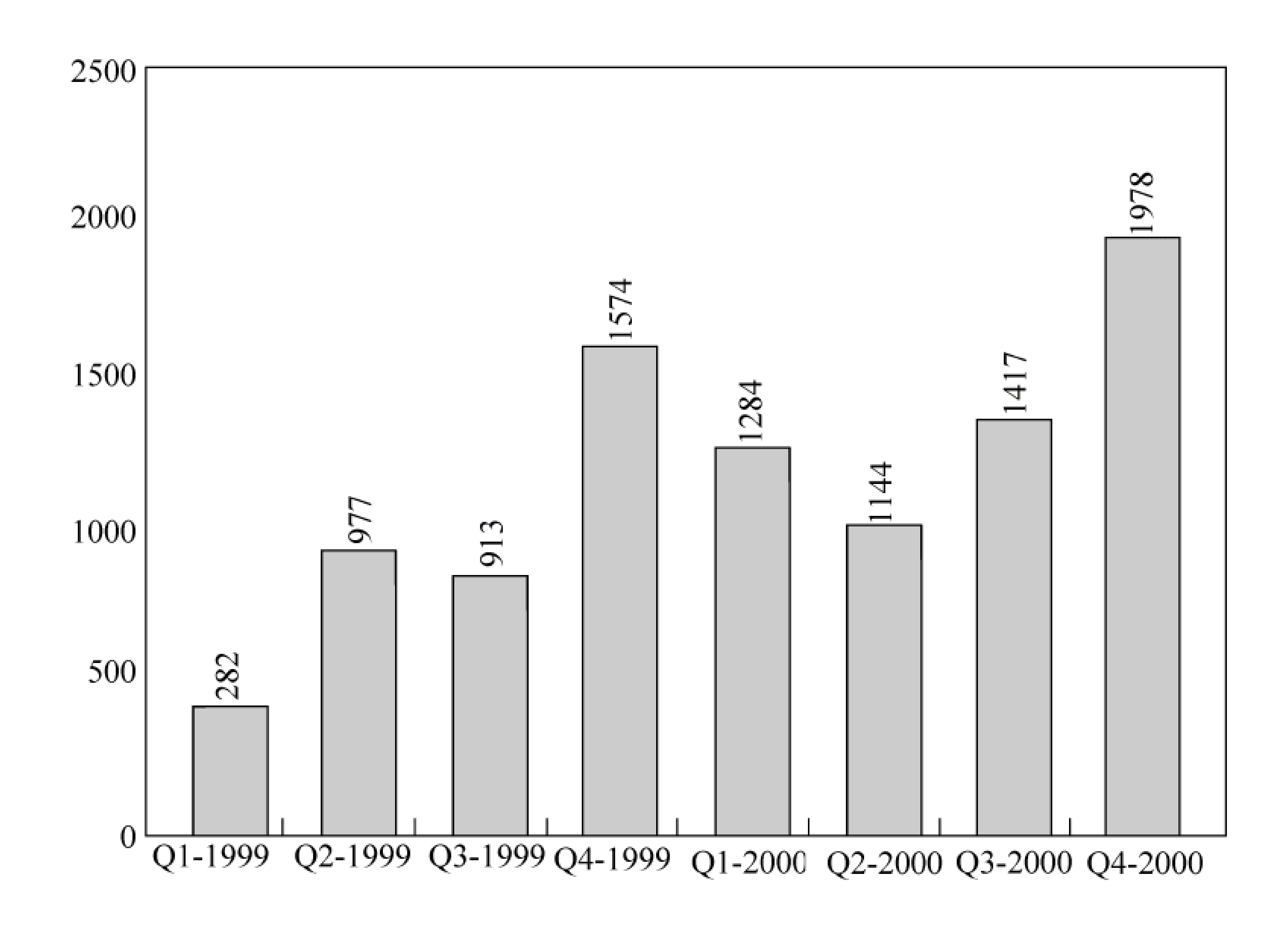


图 17-2　某公司 Web 损毁和涂改的次数

数据来源：http://www. attrition. org/mirror/attrition/annuals. html

分组回答是记录和重传网中的分组，对需要身份鉴别序列的程序是一个严重的威胁，因为入侵者可回答合法的身份鉴别序列报文，以获得系统的访问。

拒绝服务是一种损害所有可用系统资源的攻击，使系统对任何用户不可用，结果是降低或丢失服务。例如有一种攻击程序（Jolt/SSPING）可冻结任何 Windows 客户端或 Windows NT 的连接，它对被攻击的目标发送一系列欺骗的、碎片的 ICMP 分组。

特洛伊木马是一种假装有用的程序，而实际上执行非授权的有害功能。例如有一种特洛伊木马程序（SIMPSONS. EXE）看起来好像是在计算机上安装的一个程序，实际上是通过抽取将选择的驱动器上的文件删除。

病毒通常设计成能在用户计算机上复制自己的程序，无须用户计算机的任何知识。蠕虫是病毒的一种，它能在网上运行，将自己复制，并感染同一网上的所有计算机。Yankee Doodle 是一种覆盖写入常驻内存的文件感染病毒。LOVE-LETTER-FOR-YOU. TXT. vbs 是蠕虫的一个例子，它使用 Visual Basic 脚本程序的内置功能，将自己写入本地系统，并通过 Outlook 报文将自己传播出去，可进入电子邮件报文。

所有这些攻击都有一个共同点，它直接威胁一个组织的信息资产的机密性、完整性和可用性。有很多公开发表的计算机犯罪统计报告都反映了这些攻击的威胁。

当然，物理的、环境的威胁也应该在外部威胁中予以考虑。这些威胁包括停电、自然灾害、人为破坏、交通事故等。

17.1.2　内部安全威胁

根据美国 CSI/FBI 2000 计算机犯罪和安全调查的统计，在所有攻击者中，那些不满意的内部员工占的比例最高，如图 17-3 所示。

内部攻击有逻辑炸弹、特洛伊木马、非授权复制机密数据、口令探测、数据欺骗、非授

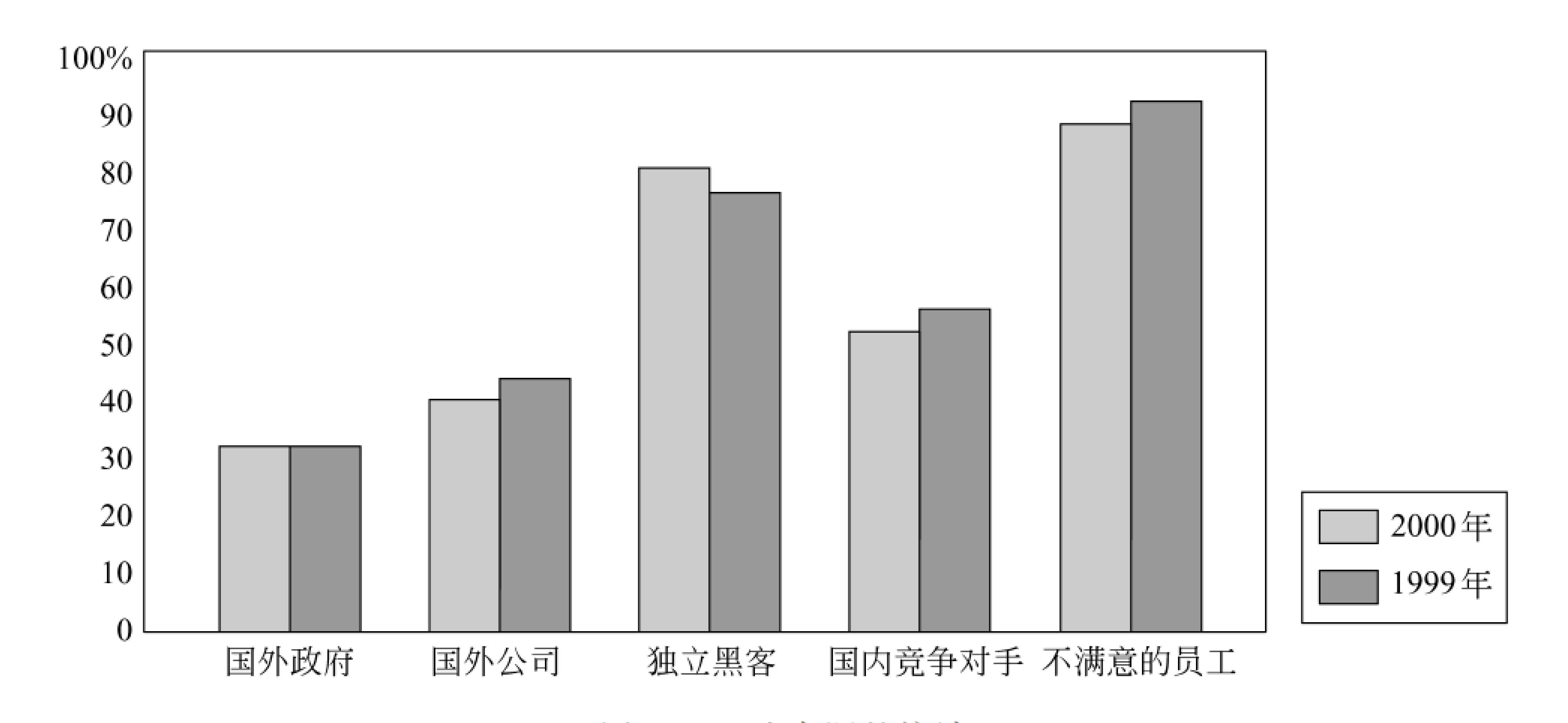


图 17-3　攻击源的统计

数据来源：美国 CSI/FBI 2000 计算机犯罪和安全调查

权软件修改、陷阱门、窃听、病毒、蠕虫等。

逻辑炸弹是最具破坏性的内部威胁之一，它是一种恶意码，设计成在特定的数据、时间或条件下执行一系列指令。数据欺骗是在进入计算机之前或之后所有关于数据的修改。口令探测是一种程序，能捕获在网上系统使用的用户名和口令信息，而那些信息正是对攻击者入侵感兴趣的。

17.2 管理安全需求

网络安全程序的成功和有效很大程度上依赖于高层管理的支持以及在组织层次结构中安全功能的配置。财经和策略的支持都来自于高层管理。为了有效，需要高层管理对信息安全功能的一些关键组成进行清晰的定义，包括管理支持、在组织中的合理布局、明确的责任和授权以及影响改变所需的资源。

网络安全必须适应各种条件的变化，包括新技术的引入、经营宗旨的变化、系统中交互会话的员工、客户、厂商的增加以及组织的成熟度等。因此网络安全程序要随着信息安全生命期（设计、布局、管理、评估）做必要的修改。

管理安全需求集中在高层管理控制，安全影响整个组织的安全结构设计和布局。运行操作和技术安全需求应全力支持管理安全需求。

17.2.1 定义安全模型

1. 信息分类等级

安全模型的核心组成是风险评估和信息分类处理。经营业务数据要根据企业的目标和组织的安全需求进行等级分类，如表 17-1 所示。

表 17-1 信息分类等级

等级名称	定 义
公共	属于可公共发布的信息，可通过合适的通道发布，如报纸、杂志、WWW、匿名服务器
内部	供内部人员知道的信息，不属于公共发布的信息
机密	企业信息，如果泄露就会对企业、客户、厂商、员工产生有害影响。这些信息在正常经营下广泛用于员工，但仅限在企业内部控制范围，在未授权情况下，不得向公众发布
严格限制	如果这些企业信息泄露，就会引起企业的财经、法律、法规或信誉的危害。这类信息是极为敏感的信息，对专门的、个别人员访问以前需要得到批准

2 经营业务影响的分析和风险评估

信息等级分类处理、经营业务影响分析和风险评估处理是相互依赖的。这些处理对组织定义安全需求起着十分重要的作用。因此，在对一个大的企业定义安全需求时，首先应完成经营业务影响分析(Business Impact Analysis, BIA)，弄明白业务功能丢失或降低的影响。企业必须标识其最关键的资产。

经营业务影响评估处理有助于减少总的信息安全代价，同时仍能保证最关键的数据得到适当的保护。如果要保护全部企业数据，其代价是很高的。BIA 标识最关键的资源以及对它们的威胁。风险评估应始于企业经营业务这个层面。通过信息搜集过程，对企业的每个经营单元，在数量和质量方面测量业务功能丢失的影响。对企业的每个经营单元填一张类似于表 17-2 的表。表中行表示经营单元的关键组件不可用的影响，列表示各个安全属性。假如一个组织的信息安全部门的用户账户删除功能不可用，那么该部门不能删除已经终断的特权用户。这就使在那个系统上的数据完整性、机密性、可用性存在风险。

表 17-2 业务功能丢失的影响

影 响 / 安全属性	15 分钟后的影响	1 小时后的影响	2 小时后的影响	1 天后的影响	3 天后的影响	1 周后的影响
机密性						
完整性						
可用性						

空格中标上高(H)、中(M)、低(L)、无(N)，分别表示对业务运行的影响大、对业务的连接运行有十分重要的影响、对业务的连续运行影响不大，以及对业务连续运行无影响。

管理安全不是容易做到的，因为难以决定风险以及同信息技术处理相关的代价。随着技术的进步，信息系统的变化，和系统相联系的风险及其安全需求也在变化。因此信息安全应周期地重新评估，并回答以下一些问题：什么是试图保护的对象？什么是组织的关键资产？这些资产的重要性如何？对这些资产的威胁是什么？这些威胁发生的概率是多少？在回答上述问题时，有什么假设条件？图 17-4 表示定义信息安全需求的框架。

17.2.2 人员安全

人员安全也是网络安全最关键的范围之一，因为员工是最终负责控制企业敏感信息

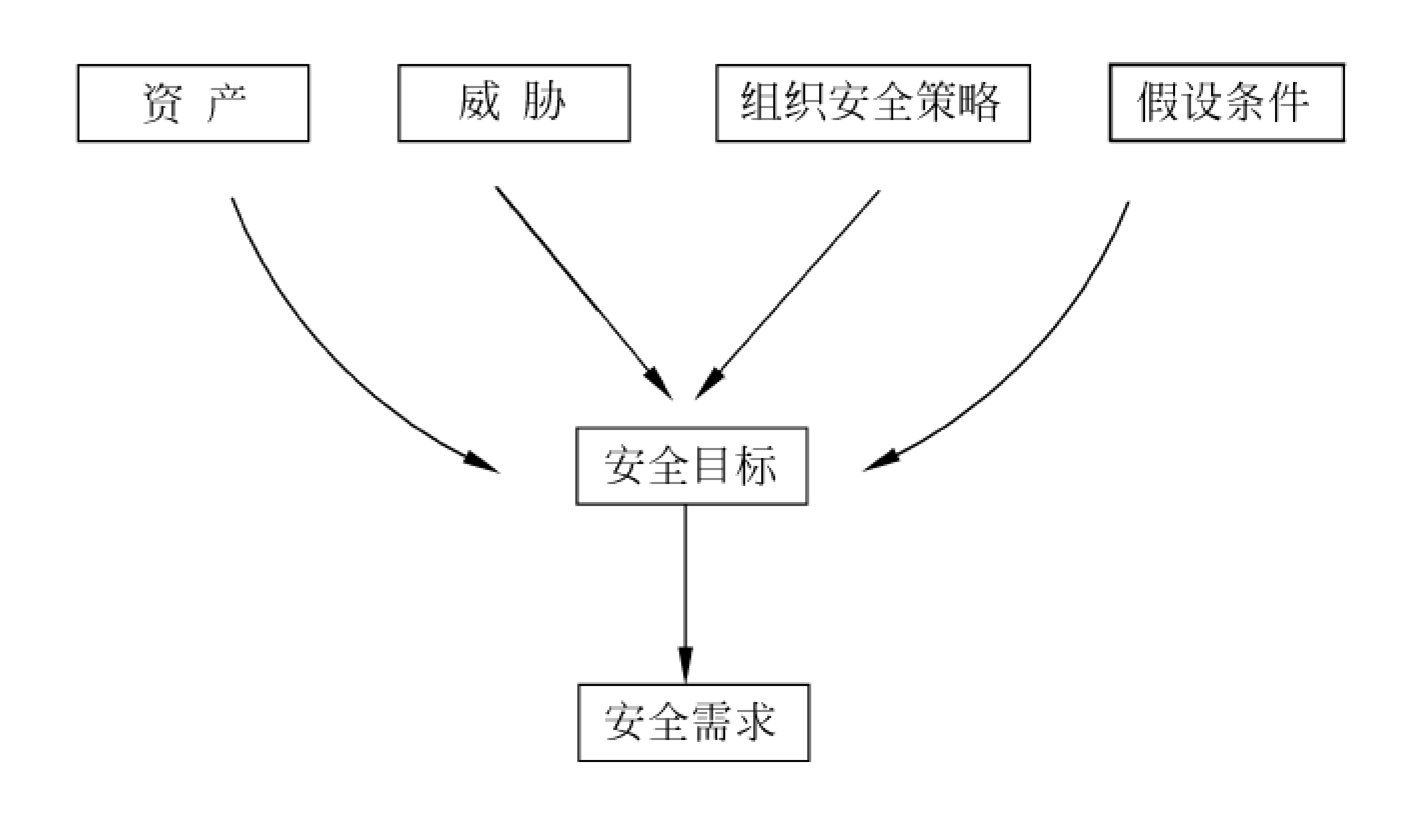


图 17-4　定义信息安全需求

的传播。对企业人员有以下一些要求：

- 企业的人力资源部必须进行员工的审查，包括其背景情况的审核，并由企业高级管理者最终审定。
- 对那些作为可信角色且有访问企业严格限制数据授权的全体员工，必须进行更加详细的背景审查，包括信用检验、犯罪记录搜索以及使用非法资产的测试等。
- 企业必须有合适的监管机制以保证角色和责任的正确执行，对所有人员进行评估，是否有足够的授权和资源来执行他们的角色和责任。
- 企业必须保证全体人员收到 1 份企业信息安全策略和知识的文本，使员工明白其责任。
- 当员工注册加入企业或离职时，人力资源部必须立即通知企业的安全部门。企业信息安全部门必须对其 ID 和口令进行注册或撤销。在员工职责变更时，也必须修改或撤销其访问。
- 当访问严格限制信息的用户授权被终止时，员工的经理应直接和系统管理员或其他相应的监管人员删除其用户访问权。

17.2.3　安全意识和培训

信息安全意识是企业培训课程不可缺少的一部分。设置和保持有效的安全意识课程，应得到各级管理的支持，而且是强制的。没有相应的管理支持，安全意识程序不可能成功。员工是保证信息安全程序有效的关键，因此他们必须明白自己在安全程序中的角色。

员工应接受常规的安全培训和提醒，安全提醒可保证信息安全策略不易忘记。信息安全培训程序可采用不同方式，然而应传递这样一个信息，即组织中的每个人都应关心安全。

企业安全培训需求阐明，必须给企业员工提供原始的（新员工）和继续不断的培训，以保持员工的知识、技巧、能力和安全意识达到有效执行所需的水平。

17.24　变更管理

应该有一个充分的过程来保证对企业资源的变更全程进行正确的实施和测试。应该提供文本来保证过程的正确进行。不一致性会引起对企业资源变更的失控，引起非授权地访问资源，并有可能让非授权人员改变安全配置程序。人员的任命变更必须是授权的，并且保持变更是可审的。企业变更管理有如下需求：

- 企业系统资源(包括硬件和软件)和支持系统必须建立文档、经过系统测试，并在执行以前进行授权。
- 所有的变更请求和系统维护必须标准化，并遵照正式的变更管理过程执行。
- 所有的变更请求必须用结构化方法来评估对资源功能可能的影响。
- 在非高峰时间进行系统维护以减少通信的影响。系统维护必须包括“滚动回退”过程，以备升级和其他维护任务失败时使用。
- 紧急处理问题必须建立文档，并由授权者通过文档管理过程来解决问题。
- 变更管理系统必须提供合适的审计跟踪设施，以跟踪事故及其发生原因。

17.25　口令选择与变更需求

口令选择与变更需求是有效安全程序中最重要的两个部分。事实上，口令是取得系统访问的最后防线。因此企业网络信息系统必须遵照以下的口令选择和变更需求：

- 用户口令必须包含至少 7 个字母、数字字符。
- 系统和管理账户的口令必须使用复合的口令，它必须由 8 个字母数字混合的字符组成，且包括大写和小写。
- 用户口令必须不含有用户名字或 ID。
- 口令不应用通信的方法给予，在口令分配和改变时，应由安全管理者直接给用户。
- 如给用户提供的是初始口令(一次性口令)，则用户第一次登录系统必须将口令改变。
- 在口令改变生效前，用户必须多次使用新的口令(至少 2 次)，以确认口令的改变。
- 用户口令重新设置必须是用户的 ID 已赋予，有关的经营单元应负责证明该用户的 ID。而新的口令必须是一次性口令。
- 用户账户的口令有效期最长必须在 60 天以内，系统和管理账户的口令有效期最长必须在 45 天以内，之后必须生成新的口令。选择同样的口令在 90 天内不能超过一次。
- 明文用户 ID 和口令必须不包括批处理登录过程。
- 用软件或硬件传递的默认口令必须立刻更换。
- 不允许用公用账户和集体口令，这样才可能在所有的时间内维护每个用户账户的可审性。
- 随着操作系统、网络设备等各种产品传递的用户账户、口令数据库和包含口令的文件，必须用适用于这些专门产品的强加密方法加密。

17.3　运行安全需求

运行安全需求致力于支撑正常经营业务运行所需的控制，运行安全涉及以下一些问题：

- 物理和环境安全控制的实施，用以保护支持企业运行的系统资源的企业设施。
- 应急和灾难恢复计划的制定，用于关键功能的连续运行。
- 应用、硬件和系统的维护控制。

17.3.1　物理与环境保护

对放置企业系统资源设施的保护控制是必需的，可以抵御物理和环境的威胁，保持连续运行。例如电源、空调、暖气、水以及其他设施的故障都可能影响电子设备的正常运行，下面列出物理和环境保护的主要方面：

- 企业的环境保护手段和控制设备必须保证企业数据中心、网络、系统的可用性和连续运行。这些手段和设备用来保护环境的各种因素(防火、防尘、电力、温度、湿度等)。必须使用烟检测器和火警系统，必须安装水监测器。
- 必须有监控器、火警系统设备测试的设施管理过程，至少每 6 个月进行一次测试，且建立测试结果文档。
- 数据中心的人员必须进行培训，使他们会使用任何自动火警系统、可携带的灭火器以及对烟和火警有正确的响应。
- 有关人员健康、安全的条件要符合国家或地区的法律、法规。
- 数据中心必须使用不间断电源 UPS 和紧急使用电源 EPS，以防止由于电源故障引起的处理环境破坏。应定期测试和维护这些设备。
- 任何时间禁止将食品和饮料带入数据中心。必须备有专门的废物存放处并定期清除。必须将各种液体远离设备。在任何时间出口和通道必须畅通。

17.3.2　物理访问控制

所有的企业信息设施应有适当的物理访问控制，防止非授权访问信息资产。本节叙述对企业的分布计算设施进行物理访问的保护需求。这些设施包括数据中心、计算机房、网络控制中心以及其他有关的区域。下面列出它们的物理访问控制需求：

- 数据处理设备的每个组件都必须是安全的，包括计算机、外围设备、终端、控制器以及其他相关设备。必须防止对计算机设备(包括服务器、路由器、交换机、通信设备等)的非授权使用，可用门锁或门卡。如果技术允许，应使用访问控制设备对成功的和不成功的访问企图做日志。
- 对大的计算机中心场地，在计算机房内对通信设备的物理访问必须进一步严格限制。

- 非本单位的人员需要访问数据中心应有书面的许可，这些访问需登记在册，且至少保持一年的记录。
- 防护门的钥匙应由负责安全的部门定期更换。
- 定期由第三方对访问控制进行考查，审计部门应委任考查组来考查访问控制和访客记录。
- 除了计算机机房的安全，还必须提供合适的大楼安全，如警卫和警门，在下班时间保护所有的设施。提供报警、闭路电视监视器、警卫、标记、仿生网络安全等，以阻止对大楼和控制区的非授权物理访问。
- 所有网络设施必须有访问控制系统的实时监控器，或者接到 24 小时运行监控站。
- 所有安全系统必须有自带的电池后备，应工作在联网环境中，必要时应有独立环境。每个系统必须有可检索的数据存档能力。

17.3.3　经营业务连续性与灾难恢复服务

经营业务应急计划（Business Continuity Planning，BCP）与灾难恢复计划（Disaster Recovery Planning，DRP）能使企业在发生重大破坏事件时保持正常的经营业务的运行。BCP 在防止可能的偶然事件以及减少由于这些偶然事件引起的对组织的危害方面起着重要的作用，它能及早采取措施以控制这些事件。DRP 在灾难发生后，标认恢复所需的关键信息，如技术应用程序、操作系统、人员、数据文件以及时间表，并选择最后采用的变更方案。BCP 和 DRP 有下面一些要求：

- 必须制定 BCP 和 DRP，且要定期测试，以保证系统的完整性和应急处理，减少由于灾难对企业造成的影响。
- 对后备和恢复必须实施综合策略管理，以保证经营业务的需求。数据中心的后备要建文档，包括每天每个服务器的增量后备以及每周的完全后备。
- 灾难恢复框架必须定义其角色和责任、所采用的方案以及计划的结构。所有在场的和离线的关键人员必须有当前的 DRP 版本，电子版本应离线存储。
- DRP 应覆盖计划和过程两个方面，包括建立通信和网络服务的过程。用来在灾难发生后，重建信息技术场地，重新开始正常的运行，且和保证员工安全的紧急过程相配合。

17.3.4　系统与应用维护

系统与应用的维护控制用来监控系统和应用软件的安装和升级。这些控制应提供保证，使系统和应用软件的选择、实施和升级不会引起处理差错或破坏基于软件的系统控制，这些控制包括以下方面：

- 系统软件选择；
- 版本控制；
- 移到生产环境前的新系统软件或现有系统软件升级的测试；
- 一旦升级失败退回到以前的版本。

在系统和应用的维护中，企业应提出如下要求：

- 在没有书面授权情况下，用于特定计算机或场地的有版权许可证的产品不应复制到其他计算机或场地。
- 只有授权的并得到企业许可的软件、硬件和设备才可使用、安装或引入企业生产环境。
- 企业的系统和应用软件应根据厂商推荐的安全补丁保持更新。系统和应用软件的当前版本具有处理和安全增强功能。校正缺陷的安全补丁由厂商通知。
- 数据中心系统软件的问题记录应标识问题的严重程度、委托专门人员分析和解决的记录以及问题的及时解决记录等。

17.3.5　敏感材料的处理

处理严格限制的、机密的内部材料时，必须防止信息不适当地泄露，为此有以下要求：

- 要生成和使用严格限制的、机密的内部信息必须安全地存储、搜集。当不需要时，必须适当地销毁和处理。
- 对严格限制的、机密的内部信息，当不需要时必须先将其切成碎片，然后抛弃。缩微胶卷必须切成小的碎片，以至抛弃后信息不能恢复。
- 用磁介质存储的严格限制的、机密的内部信息必须按下面的步骤正确处理：退磁、重新格式化、切成碎片。
- 含有严格限制的、机密的内部信息的硬复制磁介质、缩微胶卷、系统产生的报告必须严格限制再生。

17.4　技术安全需求

技术安全需求集中在对计算机系统、网络系统及其应用程序的控制。而技术安全控制的主要目标是保护组织信息资产的机密性、完整性和可用性。

17.4.1　基本安全属性需求

1. 机密性需求

机密性是保证信息与信息系统不被非授权者获取与使用。根据企业信息等级分类策略，可确定机密性的需求，如表 17-3 所示。

2 数据完整性需求

完整性是指信息是真实可信的，其发布者不被冒充，来源不被伪造，内容不被篡改。

必须保证在系统内(操作系统、硬件设备、应用系统、数据库)数据值的一致性，并要保持送到系统内部的信息和来自外部系统的信息一致性。必须保证发生系统故障时，能将信息恢复至稳定的状态。还必须保证只有授权用户和授权系统可修改数据。

表 17-3　基于信息等级分类策略的机密性需求

信息等级	机密性需求
公共	无
内部	公共通信上(Internet,拨号)传输需加密,鉴别凭证必须加密
机密	所有通信必须加密,用户工作站、台式机上的文件必须加密
严格限制	所有通信必须加密,用户工作站、台式机上的文件必须加密,仅限于授权需要知道者在企业内部通信

3. 可用性需求

可用性是指保证信息与信息系统可由授权人正常使用,确保信息与信息系统处于一个可靠的运行状态之下。

要确保信息和关键服务是可用的,以满足经营业务需求,可用性的目标是信息系统功能正常作用、数据是可用的、在丢失情况下数据易于恢复。信息可用性的影响是各种各样的,包括自然灾害和人为差错,引起系统提供的服务中断,无法获取信息,或者系统性能降低,不能及时获得信息。而必须及时得到关键的信息和服务,以满足经营业务的需求。表 17-4 是基于企业系统关键程度的可用性需求。表 17-5 是基于信息等级分类策略的可用性需求。

表 17-4　基于企业系统关键程度的可用性需求

系统	可用性(高、中、低)	系统	可用性(高、中、低)
工程网络及系统	高	市场	中
电子邮件、日程	中	远程访问和控制	中
公司电话簿	低	技术支持	中
Internet 连接	高	内部网应用	高
人力资源和工资单	高	销售和分销	高

表 17-5　基于信息等级分类策略的可用性需求

信息等级	可用性需求
公共	病毒扫描和故障在线恢复后备
内部	病毒扫描和后备/恢复
机密	病毒扫描,强的系统配置和变更管理,后备/恢复
严格限制	病毒扫描,强的系统配置和变更管理,后备/恢复

17.4.2　用户标识与鉴别

鉴别是指可靠地验证某个通信参与方是否与它所声称的身份一致的过程,一般通过某种复杂的身份认证协议来实现。身份认证是建立安全通信的前提条件,同时也是授权访问和审计记录等服务的基础。计算机系统内的鉴别包括用户标识认证、传输原发点的

鉴别、内容鉴别以及特征检测。用户可以是人、计算机系统或在另一系统执行的进程。在第 4 章已经阐述了鉴别的主要技术和方法。下面是标识和鉴别的需求：

- 每个用户应有唯一的账户。不仅要避免使用共享的账户，而且要避免在同一平台上赋予一个用户多个用户名。
- 如管理员需要综合利用通用系统，则必须给一个非管理的账户，以保证管理功能与正常的操作隔离开。
- 用户 ID 和口令必须作为一个整体来鉴别。如鉴别失败，不应给用户明确指示是用户 ID 不正确还是口令不正确。
- 所有临时的员工账户必须有一个和合同服务期相匹配的账户有效期，必须使用一个不同于正式员工的命名机制。
- 用户账户超过 60 天不活动，必须停止使用，要继续使用时，应由该账户本人提出使用账户的申请，并且提供用户标识的证明。表 17-6 是基于信息等级分类策略的标识和鉴别需求。

表 17-6　基于信息等级分类策略的标识和鉴别需求

信 息 等 级	标识与鉴别需求
公共	无
内部	用户 ID 和口令(加密的用户名、口令)
机密	强鉴别(加密用户名、口令、标记、证书)
严格限制	强鉴别(加密用户名、口令、标记、证书)

17.4.3　不可否认

不可否认的安全目标对发生的专门行为提供保证，它包括源发的不可否认、提交的不可否认以及传递的不可否认。不可否认控制防止个人否认对报文的接收、提交和传递。基于信息等级分类策略的不可否认需求如表 17-7 所示。

表 17-7　基于信息等级分类策略的不可否认需求

信 息 等 级	不可否认需求
公共	需要变更控制
内部	需要变更控制，最少的文本变更历史必须保持
机密	需要严格的变更控制，系统级文件变更历史必须保持
严格限制	需要严格的变更控制，字段级文件变更历史必须保持。需要对生成者和检查者进行数字签名

17.4.4　授权与访问控制

对用户实施鉴别后，系统必须确保用户有足够的权利来执行其请求的操作。访问控制是指确定可给予哪些主体访问的权限、确定以及实施访问权限的过程。访问控制一般

都是基于安全策略和安全模型的。第 4 章已经阐述了访问控制的主要技术和方法。通常通过系统的访问控制列表(Access Control List,ACL)来实施访问控制。它是基于各种准则来实施的,如基于用户标识、基于角色、基于时间以及基于处理等。

基于角色的访问控制十分有效。它基于请求访问用户的工作职能来决定能够访问什么样的信息,如程序员、计算机操作员、系统管理员等。职责的分离是角色和责任分开处理,以防单个人破坏关键的功能。这也是减少粗心大意或故意滥用系统的风险,以免非授权修改或滥用数据。授权与访问控制的需求如下:

- 最小特权原则。用户特权必须限制在执行赋予的职责所需的最小特权。例如,系统管理员、计算机操作员、应用和系统开发与维护、网络管理、安全管理以及安全审计各有各的角色和职能,不应将不同的角色赋予同一个人。
- 所有严格限制的、机密的内部信息和资源必须有系统访问控制,以保证这些资源不会不适当地泄露、修改或删除。表 17-8 列出了授权与访问控制需求。

表 17-8　授权与访问控制需求

信息等级	授权与访问控制需求
公共	需要修改的访问控制
内部	由经营业务单元或功能授权,需要访问控制
机密	由经营业务单元或功能授权,需要详细的基于角色的访问控制
严格限制	由经营业务单元或功能授权,需要详细的基于角色的访问控制

17.4.5　隐私

隐私(个人秘密)是当今信息经济中最重要的问题之一。组织缺乏恰当的个人秘密的惯例正在面临法律、法规和伦理的挑战。个人秘密应用到组织的信息处理中实际包括以下内容:

- 搜集有关个人(如员工、客户)的信息。
- 搜集有关个人信息的方法。
- 有关个人信息的共享。
- 搜集和共享有关个人信息的牵连。
- 能控制搜集他人信息的方法。

通常个人标识信息(Personally Identifiable Information, PII)是公共注意的中心,因为 PII 能标识和确定一个人。假如能用健康、财经、个人通信信息来标识和确定一个人,那么这些数据十分敏感,并且能进行身份标识的欺骗。生成个人秘密的经营活动包括人力资源系统管理、员工监控、电子邮件、Internet 使用、搜集个人数据的消费处理过程、直接销售、数据仓库、数据发掘以及国际数据传输等。

个人秘密与信任有关。如果组织不能对其员工和消费客户提供一个信任的气氛,就会很快破坏消费者和员工的机密。当今很多国家、地区都制定了一些个人秘密的法规。例如,欧共体于 1998 年制定了欧共体数据保护指令(EU Data Protection Directive),规定

凡是要向非欧共体国家传递个人数据，只限于那些对个人秘密保护提供合适水准的国家。

在美国，联邦政府贸易委员会(FTC)于 2000 年向国会提交了有关面向消费者的商业 Web 站点的规定。按照这些规定，在线搜集 PII 的面向消费者的商业 Web 站点应遵守 4 个广泛接受的合理的信息惯例：注意、选择、访问、安全。

对注意这一类别，Web 站点需要向消费者提供清晰的、明显的信息惯例的注意，包括搜集什么信息，如何搜集信息，如何使用搜集到的信息，如何为消费者提供选择、访问、安全，是否向其他实体泄露搜集的信息，其他站点是否通过该站点搜集信息。

对选择这一类别，Web 站点需要向消费者提供选择，除了使用已经提供的信息(例如消费者做了一次消费事务处理)外，还包括如何使用其个人标识信息。这样的选择包括内部的二次使用(例如返回消费者的市场行为)，也包括外部的二次使用(例如向其他实体泄露信息)。

对访问这一类别，Web 站点需要向消费者提供 Web 站点已经搜集到的信息的适当访问，包括适当的机会回顾信息，纠正不正确的或删除的信息。

对安全这一类别，Web 站点需要采取适当的步骤来保护从消费者搜集到的信息的安全。

以下是有关企业个人秘密的需求：

- 必须在组织内开发操作过程以确保个人秘密问题的处理。
- 必须完成一个剪裁的综合个人秘密审计程序，以提供选择，和本地区的个人秘密法规相一致。
- 医疗保健经营单位必须遵守该行业的个人秘密法规。
- 在欧洲必须遵守欧共体数据保护指令。

17.4.6 网络安全需求

企业的网络基础设施是企业的信息高速公路，它包括内部系统和外部系统。近年来，很多企业将以主机为中心的集中处理移到分布处理环境，以提供用户的 Internet 访问以及用户在家里或外出时通过拨号或虚拟专网 VPN 进入网络的能力。虽然这些分布系统为用户提供了方便和灵活性，但比传统的系统有更多的漏洞，能使非授权者入侵。将数据移到 Internet 的开放系统、更多的访问点、非集中控制以及使用混合的网络环境(如 Novell、Windows NT、UNIX 并运行 SAP、Oracle 和 peoplesoft 等)都是增加入侵的可能因素。

企业应该根据其自身的价值，定义与之相适应的网络资源有效保护水平，使网络安全与网络支持的经营业务处理一致。网络安全必须同每个应用、数据库或连到网络的平台相联系的漏洞暴露程度和风险级别相一致。以下是企业网络安全需求的内容：

- 企业网络安全应提供对分布系统的集中管理控制，在网络运行中心对多个数据中心和企业的各个场地实施安全管理。
- 企业网络进入点必须提供一个系统标题，说明系统的使用仅限于授权用户。此外，标题还应指出对非授权用户进入系统的企图会采取的行动。系统标题必须对所有试图访问企业计算机系统的用户显示。
- 所有生产网络设备，包括 LAN 服务器、路由器和交换器，必须存放在物理安全的

区域,并将房间加锁,以防非授权者进入。

- 所有同企业外公司的直接连接或专用网络连接必须得到信息安全部门的批准。
- 所有从 Internet 或外部网伙伴到企业内部网的通信必须通过企业设置的防火墙。

下面就防火墙、远程访问、安全监控与审计、平台安全以及电子邮件的安全需求做具体阐述。

1. 防火墙安全需求

Internet 和分布计算改变了组织经营业务的方法,同时也改变了网络安全的方法。企业网络不由物理边界来确定,而是由企业范围的安全体系结构来定义。防火墙作为整个安全体系结构的重要组成部分,是保护组织信息资产的一个周边防御。防火墙是在两个或更多的网络间限制访问的专门设备。第 8 章专门讲述了防火墙的功能、技术及体系结构,下面从工程的角度阐述其安全需求:

- 必须通过周边防火墙在内部网和外联网之间控制访问。必须通过非军事区(DMZ)在公共访问服务器和不能通过 Internet 直接访问的服务器之间控制访问。
- 必须在不同级别的安全和访问需求的内部网络之间控制访问,例如,账户和工资服务器同工程开发服务器之间的控制访问。
- 通过 modem 池和专门拨号网络的访问必须严格控制。
- 对第三方控制的网络的访问或来自第三方控制的网络的访问必须通过防火墙控制。
- 内部网络的地址对外部网络必须隐藏起来。
- 必须建立防火墙的文档,至少应包括防火墙的策略及包括每个规则的推理。
- 必须对防火墙和所有路由器、交换机等网络设备采用强的口令控制。防火墙和所有网络设备必须提供合适的标识与鉴别控制。防火墙的远程管理必须采用强的鉴别。
- 防火墙和路由器的配置必须能加强内部网的安全。例如,必须开发访问控制列表,尤其对具有内部 IP 地址的进入通信的访问进行严格限制。为了防止 IP 地址假冒,在路由器和防火墙产品中不允许采用源路由选择。如 FTP、TELNET、TFTP、RLOGIN 等敏感服务必须通过端口号由防火墙和路由器对进入的通信进行过滤。所有冗余的和不必要的处理必须从防火墙移去。
- 防火墙产品必须支持状态检验,而不只是简单的分组过滤。

2 远程访问安全需求

愈来愈多的企业广泛使用服务器提供的拨号 Internet 访问,为移动用户提供访问企业网资源的方法。通过诸如拨号、帧中继、ISDN、电缆 modem 或数字用户线(Digital Subscriberline,DSL)的远程访问,有可能使企业内部网受到威胁,如同受到公共网的威胁一样。为了降低这些威胁,必须有足够的控制。对远程访问的安全需求如下:

- 从 Internet 对企业资源进行远程访问时,数据机密性和完整性必须在任意时间在公共网上得到保护。
- 必须通过强的鉴别方法来确定两个端点之间的标识。远程用户远程访问系统的

机密和严格限制信息必须使用双因子鉴别。

- 直接接到个人计算机的个人通信设备的远程控制软件必须严格控制使用。
- 所有远程访问通信必须通过一个中央控制点(集中的 modem 池和防火墙)来实施集中安全管理和日志。
- 远程访问会话一旦断链,必须自动结束或重新鉴别,持续 10 分钟不活动,会话必须自动结束。
- 在 3 次无效连接访问企图后,远程访问会话必须结束,在重新设置安全管理前,必须保持不能再连接。

3. 安全监控与审计需求

安全监控是维持计算机环境安全的关键。使用企业系统的有关活动应予以监控,以保证在这些系统上的企业信息不泄露给非授权者,维护数据的机密性、完整性和可用性。监控处理包括天天监控以及使用监控安全的运行过程。这些监控活动应包括基于网络和基于主机的入侵,事件日志工具,日志检查过程,安全事件检查,定期的、实时的活动评估以及穿透测试。

系统用户和操作员要经常发现故意的或无意的旁路安全控制的新途径。安全审计日志通过记录用户活动来支持每个人的可审性。没有适当的审计机制,用户对其活动不能保持可审性,安全破坏也无法检测。

人工地检查安全特性以及解释审计日志是费时的任务。应该通过自动工具来监控。在企业网络环境中,各种设备有各种事件,如防火墙日志、入侵检测系统(IDS)事件、系统漏洞、用户审计及其在不同系统的活动跟踪。这就使得区分一个异常事件和一个严重的协同攻击十分困难。下面列出了安全监控的需求:

- 将所有安全事件合并在单一管理控制台的集中管理解决方案是必需的。这个管理控制台,可以详细检查来自各种数据源的安全事件,引出基于它们的外部事件,并生成企业安全轮廓和状态。
- 所有企业的应用、平台、数据库、网络系统或同这些系统接口的其他系统都必须提供日志能力。必须记录的信息类型包括:

  所有系统安全参数、安全轮廓、安全账户口令的改变;

  所有的特权账户(系统管理员)的改变;

  所有由特权进程、处理、程序进行的安全参数的改变;

  所有修改和删除审计日志的企图;

  所有使严格限制的和机密的数据和软件的改变;

  所有的安全违例(登录企图或口令猜测活动);

  作案者的用户 ID、事故的日期和时间、受影响的资源名、进行的活动以及设备的位置(IP 地址或最终的 ID)等信息。
- 必须保护所有的日志,以防非授权者修改、删除或读取。
- 必须记录所有拨号、基于 Internet 的远程访问,包括链接、断链、违例。
- 所有日志必须至少保留 6 个月或遵照法规的要求。

- 所有关键数据(严格限制的和机密的数据)的安全日志必须每天、每周检查。其他的日志也必须至少 2 个月检查一次。
- 基于网络和基于主机的实时入侵检测系统必须对关键应用、平台、数据库或网络进入点检测攻击或系统入侵。
- 一个计算机事故响应组(Computer Incident Response Team, CIRT)的组成应包括系统工程师、安全管理者、操作员以及 IT 人员。这个组应开发一个紧急情况事件的行动程序,例如,从网上切断已受病毒感染的机器,并且有权立即采取这些行动。响应组人员的姓名和联系方式应公布给企业的每一个员工。

4. 平台安全需求

需要保护所有硬件和软件平台,这种保护是基于它们对组织的价值以及它们的丢失可能的影响进行的。由操作系统平台执行的数据存储、处理和传输应予以保护,以防非授权泄露、修改和破坏。必须实施平台的访问控制以保护存储的数据。企业用的平台是多种多样的,比较常用的平台有用于桌面的 Windows NT 工作台、Windows 2000,用于文件和打印服务的 Novell,用于应用服务器的 Sun Solaris、IBM AIX、Windows NT 等。平台的安全需求如下:

- 平台安全必须同运行在平台上的最敏感的最有价值的应用暴露水平相一致。
- 所有平台安全设置的改变必须得到相应的系统和信息安全管理的批准。
- 只有必需的系统运行服务在平台上运行。
- 平台必须实施标准的命名惯例,以清楚地区分生产和非生产资源。
- 当一个用户获得对系统的授权访问时,系统应显示一个标题,包括用户上一次成功登录的日期和时间、最近发生的不成功登录的次数。用户必须学会观察这个标题,并向安全管理报告任何的异常。
- 所有在用户工作站和台式机上的严格限制和机密数据必须进行加密。

5. 电子邮件安全

电子邮件已经成为一个关键的和不可缺少的经营工具,用于外部和内部的通信。当处理通信的介质是数字的、全球互联的、大量的、不规则的时,可能的风险和危害的范围按指数增加。与电子邮件的使用相关联的风险,包括对商贸秘密和其他内部信息的泄露,机密客户信息的泄露,围绕性骚扰和歧视的诉讼分辨,版权侵犯的责任,非授权的评论引起的信誉损失,计算机网络被病毒和蠕虫感染。

电子邮件是企业对内、对外通信的主要方式,用来发送文件、讲话、电子数据表并 Web 连接到个人或一群人。只有授权用户才能访问和使用电子邮件资源。电子邮件通信的安全需求如下:

- 在内部和外部网上的电子邮件报文内容必须在任意时间内保持其机密性和完整性。对严格限制的、机密的内部信息必须加密。
- 电子邮件体系结构必须对源发、提交、传递提供不可否认的功能。即每个人不能否认对报文的接收、提交和传递。
- 保证天天运行的电子邮件的可用性是关键。高可用性的解决方案必须用于电子邮件的体系结构,包括电子邮件服务器和存储空间。

• 必须实施电子邮件监控，以监视不适当的内容和病毒扫描。

17.5 本章小结

网络安全需求是根据安全策略导出的。合适的安全需求可以以较小的代价控制风险，包括管理、运行、技术控制 3 方面的需求，以满足信息资产的机密性、完整性、可用性和可审性。

安全威胁可分为外部安全威胁与内部安全威胁两类。由威胁引起的损失可分成直接损失与间接损失两类，间接损失是指由于直接损失引起的后果。根据美国 CSI/FBI 的统计资料，大部分严重的经济损失来自内部的安全威胁，而间接损失又占总损失的大部分。

管理安全需求集中在高层管理控制，它会影响整个组织的安全结构设计和布局。

运行安全需求致力于支撑正常经营业务所需的控制，包括物理和环境保护、物理访问控制、经营业务应急计划(BCP)与灾难恢复计划(DRP)、用来监控系统与应用软件安装和升级的系统与应用的维护控制，以及敏感材料的处理。

技术安全需求集中在对计算机系统、网络系统及其应用程序的控制上。控制的主要目标是保护组织信息资产的机密性、完整性和可用性。

计算机系统的鉴别包括用户标识认证、传输原发点的鉴别、内容鉴别以及特征检测。应基于信息等级分类策略提出标识和鉴别需求。

企业的网络基础设施是企业的信息高速公路，它包括内部系统和外部系统。应根据其自身的价值，定义与之相应的网络资源有效保护水平，使网络安全与网络支持的经营业务处理一致，提出企业网络安全需求。

应从管理和工程角度对防火墙、远程访问、安全监控审计、平台安全以及电子邮件提出具体的安全需求。

习　　题

1. 安全威胁可分为外部安全威胁与内部安全威胁两类。由威胁引起的损失可分为直接损失与间接损失两类。根据美国 CSI/FBI 的统计资料，大部分严重的经济损失来自(　)安全威胁，而(　)又占总损失的大部分。

A. 外部，间接　　B. 内部，间接　　C. 内部，直接　　D. 外部，直接

2. 安全模型的核心组成是(　)和(　)。

A. 风险评估，安全策略　　B. 信息分类处理，安全需求

C. 风险评估，信息分类处理　　D. 上面 3 项都不是

3. (　)与(　)能使企业在发生重大破坏事件时保持正常的经营业务的运行。

A. BIA，BCP　　B. BCP，DRP　　C. BIA，DRP　　D. 上面 3 项都是

4. 技术安全需求集中在对(　)的控制上，而技术安全控制的主要目标是保护组织信息资产的(　)。

A. 计算机系统,完整性
B. 网络系统,可用性
C. 应用程序,机密性
D. 上面 3 项都是

5. 计算机系统的鉴别包括(　)。
A. 用户标识认证
B. 传输原发点的鉴别
C. 内容鉴别及特征检测
D. 以上 3 项都是

6. 什么是管理安全成功的关键和难点?
7. 企业变更管理的需求有哪些?
8. 企业网络的安全需求有哪些?
9. 什么是防火墙的安全需求?
10. 什么是远程访问的安全需求?

第18章 安全基础设施设计原理

本章要点:

- 安全基础设施定义与组成;
- 安全基础设施设计的基本目标;
- 基础设施安全服务与安全机制;
- 支撑性安全基础设施的作用与提供的服务;
- 公钥基础设施的组成及管理对象;
- 对称密钥管理的特点及关键因素;
- 基础设施目录服务的功能及重要特性;
- 信息系统安全工程的过程与方法。

安全设计需要将艺术、科学和工程集成于一体。不仅需要完全了解安全设计所保护的资产价值,而且需要预测可能采取各种方式的恶意企图。安全设计是一门艺术(技艺),需要有直观的头脑以及多年对付黑客的经验,预测很多(即使不是全部)可能的暴露点。安全设计是一门科学,设计的各个组成应是科学的、明确的,为了保护你的企业,需要丰富的知识。安全设计又是一项工程,需要用系统工程的方法,体系结构的观点,综合处理安全过程。

在完全了解所需保护的企业资产以及如何操作后,作为一个安全设计师,第一个职责是始终如一地紧跟工业实际,掌握实际动向和知识,至少要掌握最近的黑客工具和攻击技术的知识。作为安全设计师的第二个职责是设计和构造一个安全基础设施,该基础设施需要适合当前的经营业务实际,且要具有可扩展性,以适应今后的发展。在设计和集成安全基础设施前,首先要针对当前的这些威胁,并了解其发展趋势。在实施基础设施的安全技术时,应用系统工程方法将处理分成若干个子组成,确定为了保护企业资产,部署选择安全策略的方法。这些处理包括物理的、逻辑的设备安置以及这些设备运行和监控的手段。

18.1 安全基础设施概述

在阐述安全基础设施设计之前，首先必须弄懂安全设计的基本定义和组件。

18.1.1 安全基础设施的概念

一个安全基础设施应提供很多安全组件的协同使用，其体系结构可改进整个的安全特性，而不仅是各个安全组件的特性。使用这个定义，可推论出安全基础设施的设计和特性。

以防火墙为例，使用防火墙可以很好地实施安全策略，但是，如果它不能和体系结构中的其他组件很好地连接，就不能构成一个安全基础设施。例如，这个防火墙不能和安全基础设施的其他方面互相联系、互相作用，那它只是一个安全组件，而不是安全基础设施的一部分。这就是安全基础设施定义中的协同组件。再如，假如从防火墙能发送报警至事件管理站，由事件管理站处理成通知网络运行中心（Network Operations Center，NOC）的报警，那么，防火墙可能成为基础设施的一部分。反之，如防火墙本身做得很好，其屏幕可显示大部分入侵的通信，且能在搜集后做日志，但它不能通知其他任何组件，那防火墙的作用是不完全的。如果将防火墙和入侵检测、强的身份鉴别、加密的隧道（VPN）等组件协同作用，就能设计成一个基本的安全基础设施。

18.1.2 安全基础设施的组成

安全基础设施的主要组成有 4 部分：网络、平台、物理设施、处理过程。

网络类包括防火墙、路由器、交换机、远程访问设备（如 VPN 和拨号 modem 池）以及基于网络的入侵检测，它们分别在整个安全设计中增加某些安全特性。这些组件通过其网络接口或在软件中定义的逻辑来监控、过滤或限制通信。这些安全组件的作用是监控和保护在网络中通过的数据，或保护在应用中通过、使用的数据。

平台类包括服务器、客户端软件（例如，执行操作系统和安全应用的控制）。执行一些电子操作（如智能卡和读卡器、产生凭证的硬件卡、基于硬件的加密设备）的设备也属于这一类。平台类还包括应用级访问控制，如产生凭证的软件程序、数字证书、基于主机的入侵检测、病毒扫描和清除、事件搜集代理和分析软件程序。应用级访问控制能提供鉴别、授权、基于主机的入侵检测和分析、病毒检测和清除、事件账户管理和分析等功能。这些安全功能用来保护常驻在主要基础设施边界的应用。

安全基础设施的物理组成包括标准的门钥匙和锁、钥匙卡、标识标志、安全照相机、活动传感器、声像报警、安全警卫和系统、设备标签等。根据人的生物特征检测的设备也属于这一类，如指纹读出器、面部形状照相机、视网膜扫描器等。这些仿生组件是通过自然本质来标识和鉴别用户的。属于这一类的还有网络电缆和后备电源（如 UPS 系统和自备发电机）。物理安全设施的基本目的是防止非授权者进入以及保护安全基础设施的电力供应和网络连接。

处理过程包括企业安全策略和过程文档，用来管理企业数据的生成、使用、存储和销毁，以及管理这些数据所在的系统和网络。企业安全策略的目的是定义企业资产保护的范围以及对这些资产所需的专门保护机制。企业安全过程是企业安全策略文档的一个组成，用来指导员工在特定环境下的行动。企业安全策略和过程是安全基础设施的重要组成。有了综合的安全策略和过程文档，安全设计师就能明白什么样的资产是企业需要保护的，以及如何保护这些资产。

虽然安全策略文档提供数据、系统和网络的保护策略，但它对厂商选择、设计或实施并不规定所需的详细战术。这些安全组件的成功实施需要了解安全基础设施目标，否则可能会不合适地保护或完全疏忽那些关键资产。

18.2　安全基础设施的目标

安全基础设施设计的基本目标是保护企业的资产。保护这些资产的方法是适当地部署各个安全组件于有组织的、协同的安全基础设施中。这些资产包括硬件、软件、网络组件以及知识财产。保护这些资产应根据企业安全目标和企业安全策略文档。虽然提到的只是数据的保护，实际上保护数据及其可用性也意味着保护执行的系统和网络。

根据选择的数据等级分类体制，每种数据保护目标应按数据机密性、数据完整性和数据可行性来表示和衡量。

当设计一个安全基础设施时，把应用的最好结果作为目标。因为应用最靠近数据以及数据的处理、交换和存储。将设计目标放在数据机密性、数据完整性和数据可用性上，会发现这不仅使应用得到安全，而且企业也得到安全。这个概念如图 18-1 所示。

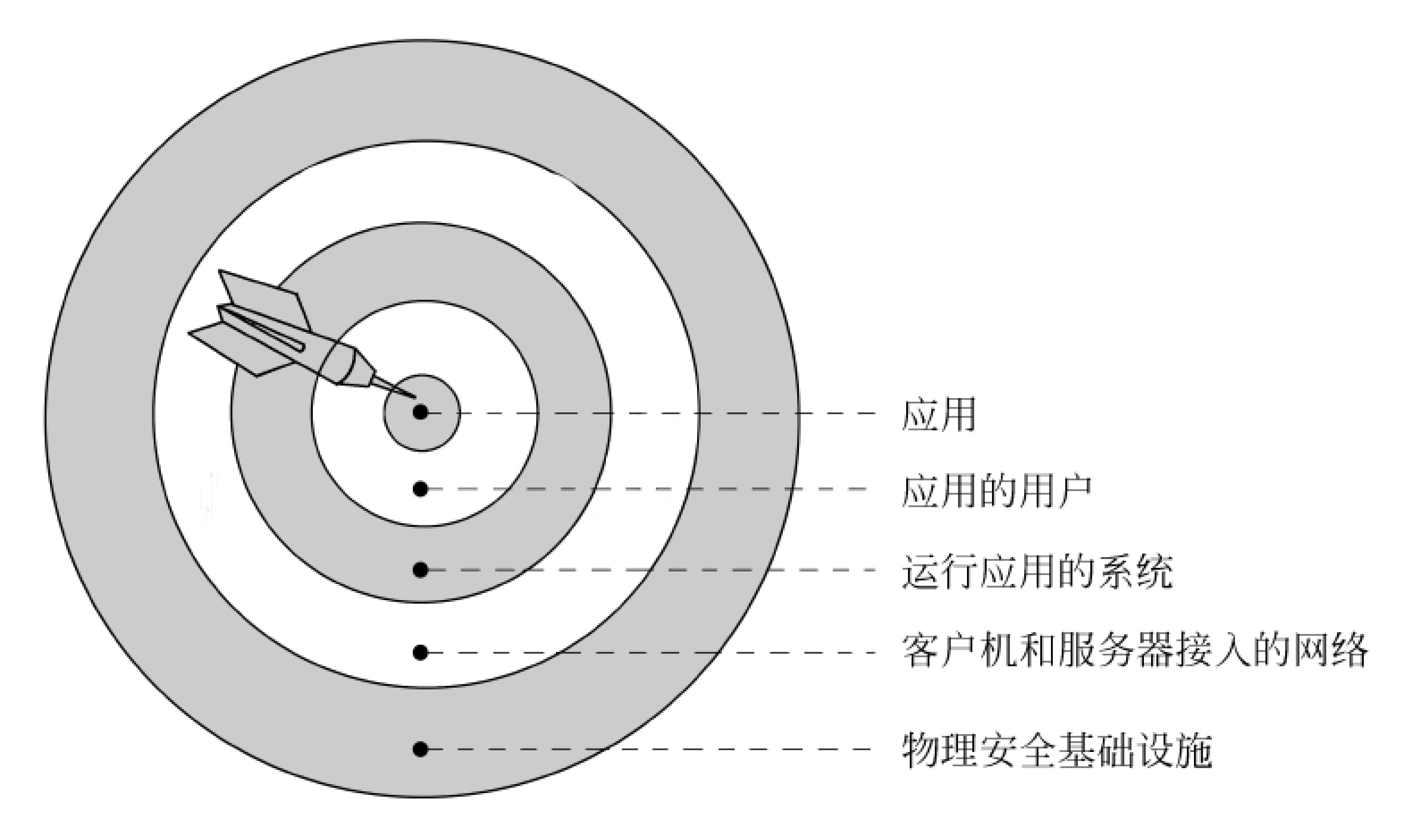


图 18-1　以应用为目标的安全设计概念

数据机密性的前提是防止非授权者看到非公共使用的数据。数据机密性应用于本书所定义的具有内部的、机密的、严格限制的标记的数据。通过安全数据存储和安全数据传输提供数据机密性保护。满足数据机密性要求的典型技术包括数据传输、安全在线和离线存储的加密。

数据完整性是关于对数据的任何非授权改变或破坏的保护。这个目标的基本点是数据的准确性和合法性。通过产生原始数据集检查和同复制的数据进行比较的程序来管理完整性。提供数据完整性的通常解决方案是使用通用的加密策略,例如前面讲到的 IPSec,使用这样的检查和策略来保证发送的数据等于接收的数据。保护数据不被更改或破坏,可以用类似反病毒这样的简单解决方法,也可以用部署关键通路存储解决方案、高可用性的防火墙簇以及企业范围的变更管理等复杂的解决方案。为了防止非授权使用或破坏,鉴别和授权控制是最合适的方法。

最后,数据可用性也是需要十分关注的。数据可用性的目标范围是根据数据可用的重要性而变化的。对某些系统需要高可用性,高达 99.999%,而有些系统可用性要求就较低。提供高可用性系统保护的典型方法是使用冗余系统,通常包括冗余的电源、数据访问和存储、网络以及应用服务器处理等。但冗余并不能满足全部数据可行性问题,尤其是近年来增多的拒绝服务(DOS)和分布式拒绝服务(DDOS)的攻击。

18.3 安全基础设施的设计指南

首先,设计指南中最重要的是要保证企业安全策略和过程与当前经营业务目标相一致。如有不一致,在设计和构造安全基础设施之前,应对这些策略和过程做必要的修改。如果设计指南没有被企业的最高管理层接受和全力支持,那么安全设计不可能完全达到它的功能,事实上有可能因缺少最高管理层的支持而失败。

第二步是开发一个计算机事故响应组(Computer Incident Response Team, CIRT),其职责是在安全报警事件中采取必要的行动和预防措施。为了使响应组成员能熟练地处理事件(如安全破坏或灾难恢复),应尽可能多地进行实际培训。在很多情况下,把它当作有目的的测试场景,在那里能测试 CIRT 成员的行动在给定安全事件下的响应、效率、完整性以及恢复能力。这样的测试目标对改进 CIRT 成员的能力是十分重要的。

第三步是设计基础设施安全服务以直接支持指南和需求。这些服务包括鉴别、授权、账户、物理访问控制和逻辑访问控制。对安全服务的设计、部署和运行应遵循专门的方法。它定义了包括评估、设计、部署和管理 4 个步骤的生命周期。在评估阶段,分析现存的经营业务和安全需求,以决定大部分实际的、有效的安全解决方案现在是否已可行,否则必须重新设计和构造。在设计阶段,针对评估中发现的问题,设计安全解决方案。部署阶段包括安全解决方案的实施和设备安装。最后是管理阶段,保证安全基础设施正常运行,功能正常。

18.3.1 鉴别

鉴别服务于 Internet 资源、外联网资源、内部网资源的用户,相应于它们内在的风险,需要不同级别的安全。内部网用户愿意基于他们登录的 ID 自动进行身份鉴别,而对外联网和 Internet 用户,需要使用赋予的硬件或软件的标记和个人标识号 PIN 登录。

通用的鉴别用户的方法包括静态用户名(UID)和口令、强的两因子鉴别、一次性口令

鉴别以及单点登录(Single Sign-On, SSO)鉴别。可能的话,为企业部署至少两种鉴别方法的组合,用于需要不同保护级别的不同等级数据。对给定类别的数据选择合适的鉴别方法是十分重要的。

最普通的鉴别方式是静态 UID 和口令的组合。因为静态口令不能经常更改,因此提供的数据保护能力是很小的。静态 UID 和口令的组合不能成功地抵御很多方式的攻击,包括回答攻击和蛮力攻击。在回答攻击中,假冒者从以前的鉴别会话中获取 UID 和口令的组合,依靠偷得的 UID 和口令给鉴别服务器回答,以得到访问权。在蛮力攻击中,攻击者只知道 UID,或使用一个默认系统账户,用很多口令和已知 UID 组合来企图登录,以得到访问权。这两种方式的攻击都广泛使用,从而削弱了静态方法的完整性。由于这个原因,只有公共数据或内部数据的访问基于静态鉴别方法。

对更高等级的数据,需要更严格的解决方法,例如,可使用强的鉴别方法和一次性口令。强的鉴别方法可使用诸如 PIN 这类的知识因子和智能卡、标记产生卡、标记软件程序等的组合。标记卡或标记软件程序使用一个算法产生通常有 6 个数字的号码,最后的口令码是该 6 个数字码和 PIN 的组合。智能卡一般包含标识其拥有的权利的信息,如数字 ID 或私钥。虽然这种鉴别方法优于静态方法,可以不再有必要用一次性口令,但大部分标记产生卡和标记软件程序利用一次性口令,使用一次后就不再有效了。很显然,强鉴别和一次性口令的组合能力大大优于静态 UID 和口令的组合,它既不会受回答攻击的影响,也不会受蛮力攻击的影响。像智能卡这些设备,当若干次非法企图后会自己失效,因此这些可携带的卡即使丢失或被偷窃,也不会有很大风险。

为了改进使用静态鉴别方法,可以建立一个口令老化的过程,规定在口令使用一定时期后必须更改。也可以在安全策略文档中规定口令加强的需求,并且在鉴别服务器中进行设定,大部分操作系统支持这种特性。

另一个设计鉴别体制时需考虑的问题是选择分布式或集中式的鉴别。分布式鉴别在业界是最流行的,对每一个要访问的系统,用户有不同的 UID 和口令,有时甚至对给定系统访问的每个应用都有不同的 UID 和口令。

与上述方法相反的是单点登录(SSO)。SSO 准许用户使用单一账号和口令的组合来访问企业中的很多资源。SSO 对用户提供方便的优点是显而易见的。它也减轻了管理的负担,管理员需跟踪的账户大大减少,由于用户忘记自己的口令而需要重新设置的负担也减轻了。

然而,SSO 不是没有一点麻烦。将 SSO 引入环境,使其在异构环境中有效地运行需要管理员付出新的努力。这些新的努力包括兼容的问题、部署和功能操作的问题,以及管理的问题等。如应用适当的智力和资源解决了大部分问题,引入 SSO 解决方案,就能成功地处理大部分企业范围的鉴别需求。

18.3.2　授权

授权是基于一个人或一个组的标识,允许或拒绝规定的特权的行为。授权应从应用的周围世界来处理。从根本上讲,应用安全是所有努力的目标。这些努力包括了解你的应用,以及如何和客户机、数据库通信,以及其他服务器处理过程。

应用通常使用一个静态的端口集以及和其他实体通信的协议。端口用来处理通信的发送和接收。决定使用什么样的端口和什么样的协议。有了这些信息，就可明白在使用哪一种应用会话方式(例如 TCP 会话)，还是通过没有会话的突发数据的应用通信(例如 UDP 或 HTTP)。明白这些应用通信类型以及如何通信有助于设计有效的、适当的授权控制。

对应用功能及其如何实现有了很好的了解后，下一步是决定谁应该在什么时间访问哪些数据，还应决定谁能得到对应用服务器、数据库或它们常驻网络段的物理访问权。这样就能防止入侵者得到访问控制。将应用访问限制在特定的群体和一天中的特定时间，就能减少受攻击的可能。

根据赋予的资源特权将用户分成组，通过按资源将用户分组的方法，用赋予的组标签在应用级进行授权控制来控制组成员的活动。这样的策略是基于角色的访问控制(role based access control，RBAC)。虽然 RBAC 控制很好，适合于具有大量用户和大量公共或内部数据资源的服务，但是对标有机密或严格限制的数据保护需要更严格的控制。基于用户的访问控制(User Based Access Control，UBAC)是根据各个用户的特权而不是赋予的角色来决定的访问控制。UBAC 需要对每个用户分别进行鉴别和授权。UBAC 控制从其本性看可提供更细粒度的控制，因为它直接应用至每个用户或单个实体，而不是组或多个实体。

18.3.3　账户

账户管理涉及日志和行为的监控、事件以及满足某些条件引起的报警。大部分操作系统能配置生成账户日志，对各种系统里发生的事件向管理者发出报警。最流行的操作系统日志程序是用于 UNIX 系统的 Syslog 和用于 Microsoft NT 的 NT 事件日志。UNIX Syslog 或 NT 事件日志设置报警，在日志文件中产生报警级报文，或更高级的报文。然而，情况可能更为复杂，如若干个相关的、协同的、不一样的事件从不同的代理源发生，其结果是发出更严重的报警信息。不论复杂性如何，账户管理结果都能提供以下信息：

- 操作系统使用的详细情况；
- 应用使用的详细情况；
- Internet、外联网或内部网的活动；
- 用于法庭分析的数据；
- 趋势分析数据；
- 生成报告的数据。

这些结果对企业都是很有价值的。除了提供性能预测和趋势分析之外，这些事件还能确定它的安全轮廓、标识存在的或可能的威胁。操作系统事件能提示安全职员下列情况：失败的登录企图、企图得到根或管理员的访问、文件系统是否已被安全送出。

事件的时间界限和事件覆盖的范围一样重要。当管理员只是每周一次用人工方法考查事件日志时，从操作系统、关键应用以及在网络段上的通信监控安全事件到底有多少价值呢？当管理员周期地考查这些事件日志，查看一段历史时，黑客和漏洞的跟踪有可能早

已离开了,一些关键数据也可能已被取走。

在 Internet 年代,事情发生得很快。即使是黑客新手也可能用大量黑客工具来攻击企业资产。这些新手从专门黑客那里得到好处,裁剪黑客工具对企业施加严重的破坏。

因此,不仅需要连续的访问和鉴别控制,还需要实时的事件管理和入侵检测(ID)解决方法。将入侵检测也作为账户管理解决方案的一个组成部分,因为它的自然特性是事件检测、分析,还有防止,十分类似于事件管理的目的。以往只是将事件管理当作一种静态搜集信息的工具,在这里将事件管理作为一种实时安全报警机制。

18.3.4 物理访问控制

物理访问控制有关安全基础设施的组件,和其他安全设施一起减少资源滥用的效应。物理控制的操作是物理的。

通用物理访问控制包括标准的门钥匙、钥匙卡、标识标志、安全照相机、活动传感器、声像报警、安全警卫和系统、设备标签等。使用这些组件的方法决定了物理访问控制策略的质量。企业安全策略和过程文档定义的操作应定义如何保护专门等级的数据及执行的系统。这些过程还应陈述在灾难事件中通知相应的人员采取哪些行动,对应用重要的数据影响,定义相应的法庭过程以及如何降低相关的风险。

除了减少安全漏洞的风险和影响外,服务的破坏也必须计入物理保护策略。服务破坏保护策略包括正确的组件放置以及冗余。安全基础设施放置和冗余是一样重要的。例如,某公司需要一个高可用性的系统和数据为客户服务,为此公司需安装一条冗余的 T-1 电缆接到提供客户服务的数据中心,同时需要安装冗余的 UPS 设备。由于施工土建工作量较小,施工过程未同土建安全部门联系。但这种疏忽有可能会引起水、电等事故,这类事故在安装物理基础设施组件时本来是完全可以避免的。

18.3.5 逻辑访问控制

逻辑访问控制是所有安全基础设施控制中最引人注目的。这些控制包括防火墙、路由器、交换机、VPN 和应用层控制,用来限制系统和网络的使用。如前所述,逻辑访问控制有时使用鉴别和授权信息来决定准予或拒绝访问。另外,这些决定取决于正在使用的端口和协议。这些控制最好先集中在应用上,然后再控制低层协议。

下面举例说明,假定有一个 HealthApp 的应用,此应用利用端口 8111 上的 TCP 和 HealthApp 客户通信,而 TCP8104 处理服务器对服务器的通信。首先需明白应用的功能,而不是一开始就访问控制不希望的端口和协议。在本例中,HealthApp 服务器和其他服务器通信首先执行一个域名系统(DNS)的查找来发现要同它通信的服务器的 IP 地址,HealthApp 服务器和 DNS 服务器之间的 DNS 询问必须是允许的。

在本例中,下一步是对不是和 HealthApp 应用相联系的操作,拒绝所有访问控制设备(例如防火墙、路由器、交换机)上的通信,并对应用进行测试。这样以应用为目标,导出可用的、最安全的逻辑访问控制集。可以发现,使用这个策略是保护应用数据及其执行的系统的最有效方法。

逻辑访问控制能应用不同的方法来限制系统和网络的使用。对应用访问的保护，逻辑访问控制通常使用在应用本身。基于鉴别和授权准则，可设计成明确的限制或允许一定用户或用户组的访问。网络访问控制根据试图经过一个网络段的端口号和协议来决定允许还是拒绝通信。很多防火墙、路由器、交换机、VPN 网关和 ID 系统可以根据它的类型（TCP、UDP 或 IPX）、源、目的甚至载荷来限制通信。

逻辑访问控制通常最后使用入侵检测系统，包括发送一个 TCP RESET（RST）分组给非授权网络通信的发送源。这个 RST 分组通知发送源（冒犯者）的主机该数据会话没有接收到。虽然这个冒犯者的主机可能继续再试，但它的非授权通信经过给定的网络段，入侵检测系统将重新设置这个会话，因此阻止了该通信到达目的站。

实践证明，最好的逻辑访问控制实施策略是包括周边的建立、内部应用和基于网络的控制、基础设施的保护。周边的建立将决定哪些系统和网络是最可信的（内部的），哪些系统和网络有点可信（DMZ），哪些系统和网络根本不可信。图 18-2 表示建立可信域的模型。

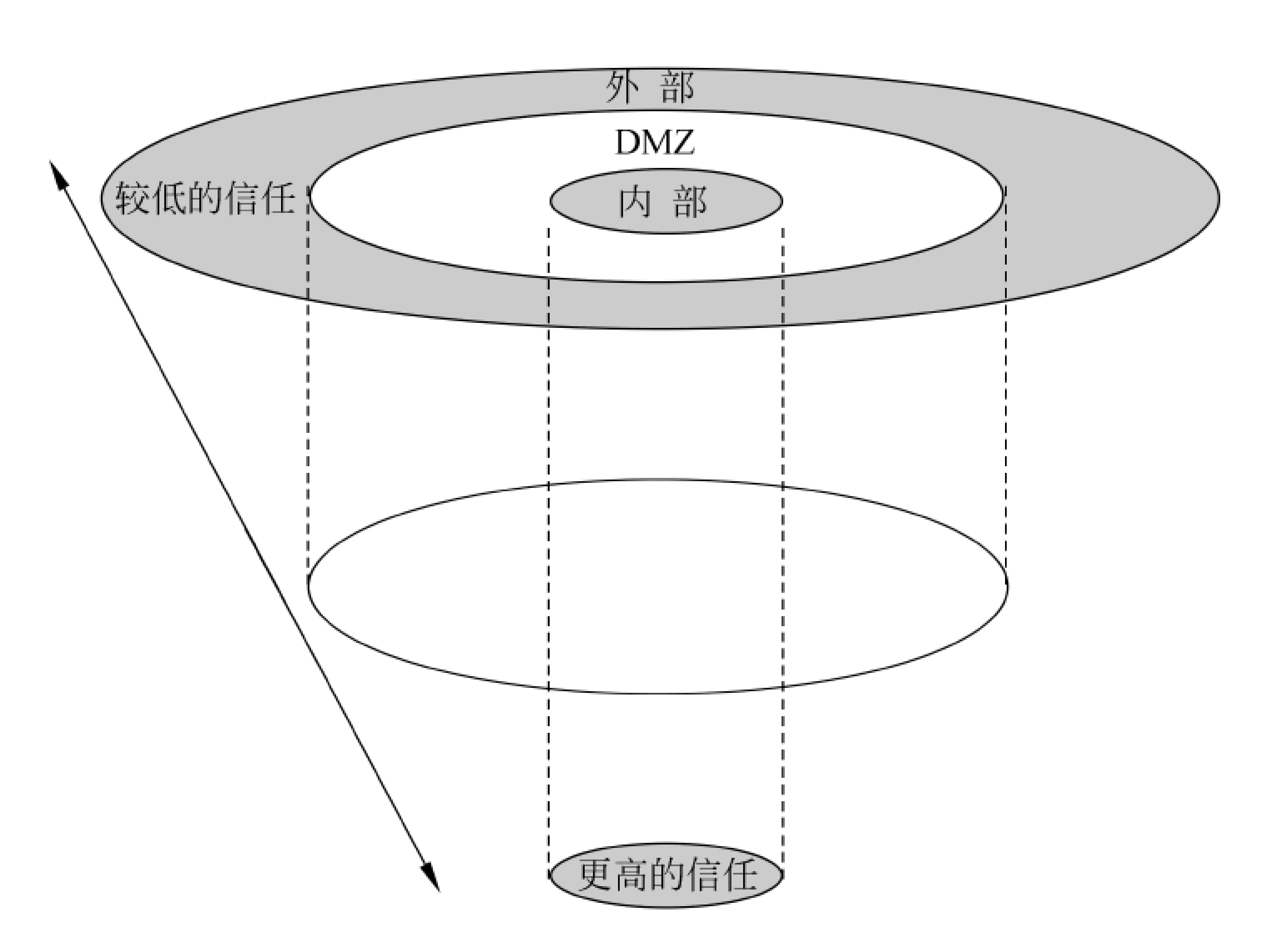


图 18-2　可信域的模型

设计分开的可信区域，就能使用访问控制，以适合不同可信区域内网络和系统的经营业务的目的。Internet 需要和内部网和外联网不同的访问控制水平，不仅必须选择合适的访问控制技术，还必须包括基础设施的正确部署位置。入侵检测系统安装在周边防火墙内和防火墙外结果不同。不仅重要的事件及其内容不同，而且使用的数据机密性、完整性和可用性的需求也不同，事件着重点的改变也相当大。

当实施这些控制时，应尽可能少地牺牲企业的生产力和利益，这是必须考虑的因素，虽然要做到这点不容易。

18.4　密钥管理基础设施/公钥基础设施

支撑性基础设施是能够提供安全服务的一套相互关联的活动与基础设施。有两个十分重要的支撑性基础设施：

- 密钥管理基础设施/公钥基础设施，用于产生、公布和管理密钥与证书等安全凭证。
- 检测与响应，用于预警、检测、识别可能的网络攻击，做出有效响应以及对攻击行为进行调查分析。

本节阐述密钥基础设施与公钥基础设施（KMI/PKI），KMI/PKI 作为一种支撑性基础设施，其本身并不能直接为用户提供安全服务，但 KMI/PKI 是其他安全应用的基础。KMI/PKI 是安全服务所必需的组件，其体系结构依赖于其支持的应用。表 18-1 列出了不同用户类型对 KMI/PKI 的需求。例如，在为两个用户提供端到端加密隧道的虚拟专用网（VPN）中，KMI/PKI 为实现认证和加密功能的加密设备提供密钥和证书，还为用户提供密钥恢复服务以及证书查询的目录服务。

表 18-1　KMI/PKI 支持不同类型的用户服务

用 户 类 型	KMI/PKI 服务			
VPN	密钥产生	证书管理	密钥恢复	目录服务
网络访问控制	密钥产生	证书管理	增值服务	目录服务
远程访问服务	密钥产生	证书管理	密钥恢复	目录服务
多级安全	密钥产生	证书管理	目录服务	

与其他基础设施解决方案不同的是，KMI/PKI 将它的安全分布在一组独立的组件上。这些组件本身比用户应用要求更高的安全性，以保证用户证书和密钥的安全性。同样，基础设施中的安全策略管理、信息保障的水平等都要高于用户应用的安全级别。

18.4.1　KMI/PKI 服务

为了减少用户获取服务的成本和需花费的人力资源，要求将提供不同服务的支撑性基础设施组合在一起，形成一个能为用户提供多种服务的多组件基础设施。KMI/PKI 支持 4 种服务，其中每一种服务都使用了多种机制来满足用户应用对安全的不同要求。前两种服务能直接支持用户应用，后两种服务是用户应用正常工作所必需的。

第一种服务是对称密钥的产生和分发。对称密钥的产生和分发仍然是政府部门、金融部门和密钥管理机制中最主要的部分。尽管许多应用正在使用非对称密钥管理代替对称密钥管理，但对称密钥管理仍然有用武之地。对称密钥中，多个用户的密钥的产生、分发和管理由一个中心（可能是一个用户或一个独立的第三方）完成。在应用对称密钥的团体中，一个成员在其密钥的生命周期中只使用同一个密钥与其他成员进行保密通信。

第二种服务是支持非对称密钥技术及与其相关的证书管理。非对称密钥通常使用数字证书来鉴别公/私钥对中公钥部分的真实性。这种鉴别很重要，因为非对称密码提供的安全服务要依赖于公钥用户确保公钥已与特定的用户绑定。数字证书（X.509 证书）恰恰

能将公/私密钥对中的公钥部分与其拥有者的身份绑定在一起，并使用密码技术保证这种绑定关系的安全性。公钥基础设施由多个部分组成，包括组成基础设施的组件、使用并操作基础设施的人员、基础设施提供的服务、基础设施运行的策略以及对公钥证书的管理。公钥基础设施可以产生、管理数字证书以保证数据的真实性、完整性及不可否认性，也可产生、管理密钥协商证书以保护数据的机密性。

第三种服务是目录服务。通过目录服务，用户可获得 PKI 提供的公开信息，如公钥证书、相关基础设施的证书、受损的密钥信息等。目录服务可以由全球的分布目录集提供，如 X. 500DMS(Defense Message System)，也可以由单一站点组成的在线存储库提供。目录服务一般与 PKI 结合在一起使用，但也可以用来提供其他服务。

第四种服务是对基础设施本身的管理。基础设施是由多个组件协同工作为用户提供服务的，这种分布特性增加了对 KMI/PKI 的功能和操作上的要求。同时应用安全需求的敏感性也对 KMI/PKI 提出了更多的安全需求。KMI/PKI 的内部结构也受其支持的应用的影响。

KMI/PKI 能支持不同的安全应用，这取决于应用使用的密码技术。对称密码技术一般保护信息在传输和存储中的机密性，如传输机密性、文件加密、密钥协商。对称密钥技术与其他机制相结合也可保证交易过程中数据的完整性和真实性，从而确保交易安全，如鉴别、完整性、不可否认等安全应用。与对称密码不同，非对称密码技术可以保护信息在传输和存储中的完整性和真实性，如鉴别、完整性和不可否认等安全应用。公开密钥密码技术与证书管理相结合可以为应用提供全方位的安全服务。公开密钥密码技术对数据进行加密、解密的速度比较慢，因此一般都使用对称密码算法对数据进行加密和解密。

18.4.2　KMI/PKI 过程

KMI/PKI 包含一系列过程。这些过程需要正确地协同工作，以保护用户服务的安全。这些过程列举如下：

① 注册。在系统中登记已经过认证的用户，使其可以使用 KMI/PKI。

② 申请。用户向 KMI/PKI 请求密钥或证书。

③ 密钥生成。由基础设施的一个组件产生对称密钥或不对称密钥。

④ 证书生成。将用户的信息和用户的公开密钥绑定在一个证书中。

⑤ 分发。通过一种安全的可认证方式将密钥和证书分发给用户。

⑥ 审计。记录密钥和证书的位置和状态。

⑦ 受损恢复。通过一种可验证的方式将无效的密钥和证书从系统中删除。

⑧ 密钥更新。以一种安全的可认证方式周期性地更新密钥和证书。

⑨ 销毁。销毁失效的私钥。

⑩ 密钥恢复。不直接访问用户私钥的复制而恢复用户私钥的能力。

⑪ 制定策略：定义上述操作的应用需求。

⑫ 管理：运行基础设施。

⑬ 增值 PKI 过程。提供一些可增值的服务，如备份、时间戳、公证等。这部分不是必需的。

在 PKI 中，由不同的组件负责处理不同的操作。上述的操作可以有多种方法进行组

合，为用户提供安全服务，具体的实现方式依赖于具体的应用和用户愿意投入的成本。KMI/PKI 的整体安全由各个操作的安全性构成，每一个操作都面临着不同的攻击威胁并有相应的防范措施。表 18-2 定义了 4 种 KMI/PKI 服务对实现每一个操作的基本要求。

表 18-2　KMI/PKI 操作

操作	证书（公钥）管理	对称密钥管理	基础设施目录服务	基础设施管理
制定策略	N/A	N/A	N/A	定义域中的策略以及执行策略的方法
注册	在系统中登记合法用户	登记经过认证的可以申请密钥的用户	登记有权更新目录的用户	向基础设施中增加新的处理认证操作的组件，如交叉认证
申请与验证	• 证书中信息的有效性 • 验证密钥产生请求 • 接收公钥	验证申请密钥请求	验证信息请求	• 验证改变信任模型的过程 • 接收基础设施组件的公钥
产生	• 产生公/私密钥对 • 产生证书	产生密钥	向目录中增加信息	• 产生根公/私密钥对 • 产生根证书 • 产生基础设施组件的公/私密钥对 • 产生基础设施组件的证书 • 产生交叉认证证书
分发	• 向用户提供证书 • 验证获取证书的用户是否具有相应的私钥 • 将策略批准权威（PAA）的公钥证书通过可认证的途径发送给用户	• 将密钥发送给用户 • 将密钥装入到加密设备中	向用户提供信息	• 通过安全的途径将根证书提供给基础设施的各个组件 • 为每个基础设施组件提供证书 • 确保每个基础设施组件拥有公钥对应的私钥 • 通过安全的方式向基础设施组件提供域内的加密参数
受损恢复	• 对失效的密钥提供失效密钥列表（CKL） • 对处于有效期内的证书提供在线认证机制	取消所有使用失效的密钥的密码设备	修复一个受到攻击的目录	提供整个基础设施或组件失效或遇到灾难后的重建步骤
审计	在密钥和证书整个生命周期内跟踪其位置和状态	在密钥的整个生命周期内跟踪其位置和状态	记录何人何时修改目录中的信息	确保对基础设施的组件的操作符合 PAA 定义的策略和操作流程
密钥恢复	适当的密钥恢复机制	N/A	N/A	根签名密钥可能需要密钥恢复

续表

操作	证书(公钥)管理	对称密钥管理	基础设施目录服务	基础设施管理
密钥更新	• 新证书 • 新密钥	密码设备的密钥更新	N/A	改变根密钥的过程
销毁	到达私钥使用期限后将其置 0	达到密钥使用期限后将密钥置 0	将信息从目录中删除	到达基础设施组件的私钥使用期限后将其置 0
管理	N/A	N/A	N/A	安全地使用基础设施组件和运用系统策略的操作步骤

18.4.3　用户和基础设施需求

1. 用户需求

(1) 对称密码

- 密钥的来源应该是可信的、权威的、可鉴别的;
- 在分发过程中应该对密钥进行保护。

(2) 非对称密码

- 由用户或 KMI/PKI 来产生公/私密钥对;
- 证书信息是准确、有效的,并反映了与可识别的唯一用户之间有效的绑定关系;
- 证书将用户私钥对应的公钥与用户身份绑定在一起;
- 可信基础设施组件的证书通过可鉴别的方式传递给用户;
- 用户可以周期性检查证书中信息的有效性;
- KMI/PKI 只为在策略中定义的经过认证的实体(如用户或用户组织)提供数据恢复服务,例如提供私钥的一个复制。

2 基础设施管理需求

(1) 对称密码

- 确保密钥产生和分发的请求者经过认证;
- 密钥产生过程是安全、强健的;
- 在密钥分发过程中保证密钥的安全性;
- 密钥只分发给经过认证的用户;
- 系统要对密钥整个生命周期进行审计(申请、产生、分发、使用、更新以及销毁);
- 系统要将失效的密钥从系统中删除。

(2) 非对称密码

- 确保证书申请的发起者经过认证;
- 产生证书之前确保证书申请中的信息与用户的实际情况相符合;
- CA 要保证将正确的公钥写入证书中;
- 如果系统为用户产生公钥,则要保证密钥产生的安全性并安全地传递给用户;
- 基础设施要确保其证书的完整性,并以可鉴别的、不可否认的方式传递给用户;

- 基础设施必须周期地为用户提供证书撤销信息；
- 基础设施必须保证其组件的高可用性；
- 系统对密钥的生命周期进行审计(申请、产生、分发、应用、更新、撤销和归档)；
- 基础设施只对已认证的用户或用户组织提供私钥的恢复机制；
- 基础设施存储的密钥要使用密钥恢复机制保护密钥；
- 保证恢复的密钥在分发给用户的过程中的安全。

3. 互操作需求

注意：密钥管理基础设施之间的互操作性并不保证用户应用之间的互操作性。

(1) 对称密码

- 能够将密钥和密钥受损信息分发给所有的用户；
- 分发给用户的密钥格式要统一；
- 对所有用户的密码算法和初始化参数一致。

(2) 非对称密码

- 进行交叉认证的 PKI 之间要认证各自的策略；
- 用户可以从多个安全域中获取证书；
- 基础设施需要支持多种加密算法，用户可以选择对其证书签字的算法；
- 统一的密钥和证书格式，如证书采用 X.509 定义的证书格式；
- 统一用户使用的算法和初始化参数；
- 所有的用户都能得到受损恢复信息。

18.5 证书管理

KMI/PKI 的一个主要功能就是对使用公钥的应用提供密钥和证书的产生、分发和管理服务。在 KMI/PKI 的分工中，PKI 的目的就是管理密钥和证书。本节从用户的角度出发介绍 PKI 的功能及其体系结构。

为了给各种基于公钥的应用提供服务，PKI 的组成包括一系列的软件、硬件和协议。PKI 的主要组成部分包括证书授权(Certification Authority, CA)、注册授权(Registration Authority, RA)以及证书存储库(Certificate Repository, CR)。PKI 管理的对象有密钥、证书以及证书撤销列表(Certificate Revocation List, CRL)。下面简要介绍这些组件。

- CA。被一个或多个用户信任并负责创建、分发证书，操作 CA 的人称为管理员。
- RA。负责认证 CA 申请证书的用户身份的实体。RA 并不签发证书，一般位于离用户比较近的地方。完成 RA 认证用户这项任务的人称为 RA 操作员。在大多数 PKI 中，完成认证用户身份的任务一般由分散的、离用户较近的局域注册授权(Local Registration Authority, LRA)完成。

- CR。CA 发布证书和 CRL 的地点。存储库有多种实现方式，包括数据库、Web 服务器，但一般用户都使用 LDAP 协议访问目录服务。
- 非对称密钥。非对称密钥算法中需要一对密钥，一个用来加密、签字，一个用来进行解密、验证。密钥对中有一个是由密钥拥有者秘密保存的，称为秘密密钥，另外一个由密钥按照一个不可逆的数字函数计算得到，并可公开，称为公开密钥。根据数学原理，由公开密钥不可能推导出秘密密钥，所以公开密钥不会影响秘密密钥的安全性。
- 证书。将用户的身份信息及其公钥用一种可信的方式绑定在一起的一条计算机记录。证书中包括签发者名称、用户身份信息、用户公钥以及 CA 对这些信息的签字。目前多数证书格式都遵循 ITU X.509 标准定义的证书格式，凡符合X.509 标准的证书称为 X.509 证书。
- CRL。包含尚处于有效期内、但证书内的用户身份信息及其公钥的绑定关系已经失效的证书列表。CRL 由 CA 签发，CRL 可以通过多种方式发布，如发布到目录服务器中，利用 Web 方式发布或通过 E-mail 方式发布。

同其他 PKI 相联系的、处于不同保护地址中的通信实体，如果信任报文发送者的证书签发者 CA，那么可以对报文发送者的证书进行鉴别。如果用户相信 CA 能将用户身份信息与公钥正确地绑定在一起，那么用户可以将该 CA 的公钥装入到用户的加密设备中。可以用用户信任的 CA 公钥验证其签字的，并且不在 CA 签发的撤销列表中的任何证书都是有效证书。这意味着用户可以从该证书中解析出公钥，并相信该公钥确实属于证书中标明的用户。

大型公钥基础设施往往包含多个 CA，当一个 CA 相信其他的公钥证书时，也就信任该 CA 签发的所有证书。多数 PKI 中的 CA 是按照层次结构组织在一起的，在一个 PKI 中，只有一个根 CA，在这种方式中，用户总可能通过根 CA 找到一条连接任意一个 CA 的信任路径。

在采用层次结构的组织中，层次结构的 CA 组织方式非常有效，但对于内部不采用层次结构的组织以及组织之间，则很难使用层次结构的 CA 组织方式。解决这个问题的一个很通用的方法是，将多个 CA 证书结构内受信任的证书安装到验证证书的应用中，大多数商用浏览器中包含有 50 个以上的受信任的 CA 证书，并且用户可以向浏览器中增加受信任的 CA 证书，也可以从中删除不受信任的证书。当接收一个证书时，只要浏览器能在待验证证书与其受信任的 CA 证书之间建立起一个信任链路，浏览器就可以验证证书。

另一种方法是双向地交叉认证证书。采用交叉认证不像层次结构组织 CA 的 PKI 那样，需要在 CA 之间建立上下级的信任关系。为了区别于层次结构的 PKI，采用双向交叉认证机制的 PKI 称为网状 PKI。层次结构的 PKI 可以同网状结构的 PKI 组合在一起。在层次 PKI 与网状 PKI 之间进行互操作可采用桥 CA 的概念，桥 CA 为多个 PKI 中的关键 CA 签发交叉认证证书。

不论是采用层次结构还是采用网状结构的 PKI，签字的验证者必须建立一条从签字

者到验证者信任的 CA 之间的证书链，验证者必须验证证书链中的每一个证书的签字，并检查该证书是否已经撤销，如果证书链中的每个证书都是有效的，那么验证者可以确认签字者的公钥是有效的。

不使用证书链对证书进行验证的方法称为在线证书验证。在线证书验证的过程是将证书传递给网络上的服务器，让该服务器根据其验证规则来实现对证书有效性的验证。

图 18-3 表示 PKI 互操作中的分层信任列表与网状方法。图 18-4 表示基于双向交叉认证、桥 CA 和在线状态检查互操作模型的 PKI。在多个 PKI 间进行互操作的方法都各有其优缺点，必须仔细考虑选用互操作方法，以防降低系统的安全性。

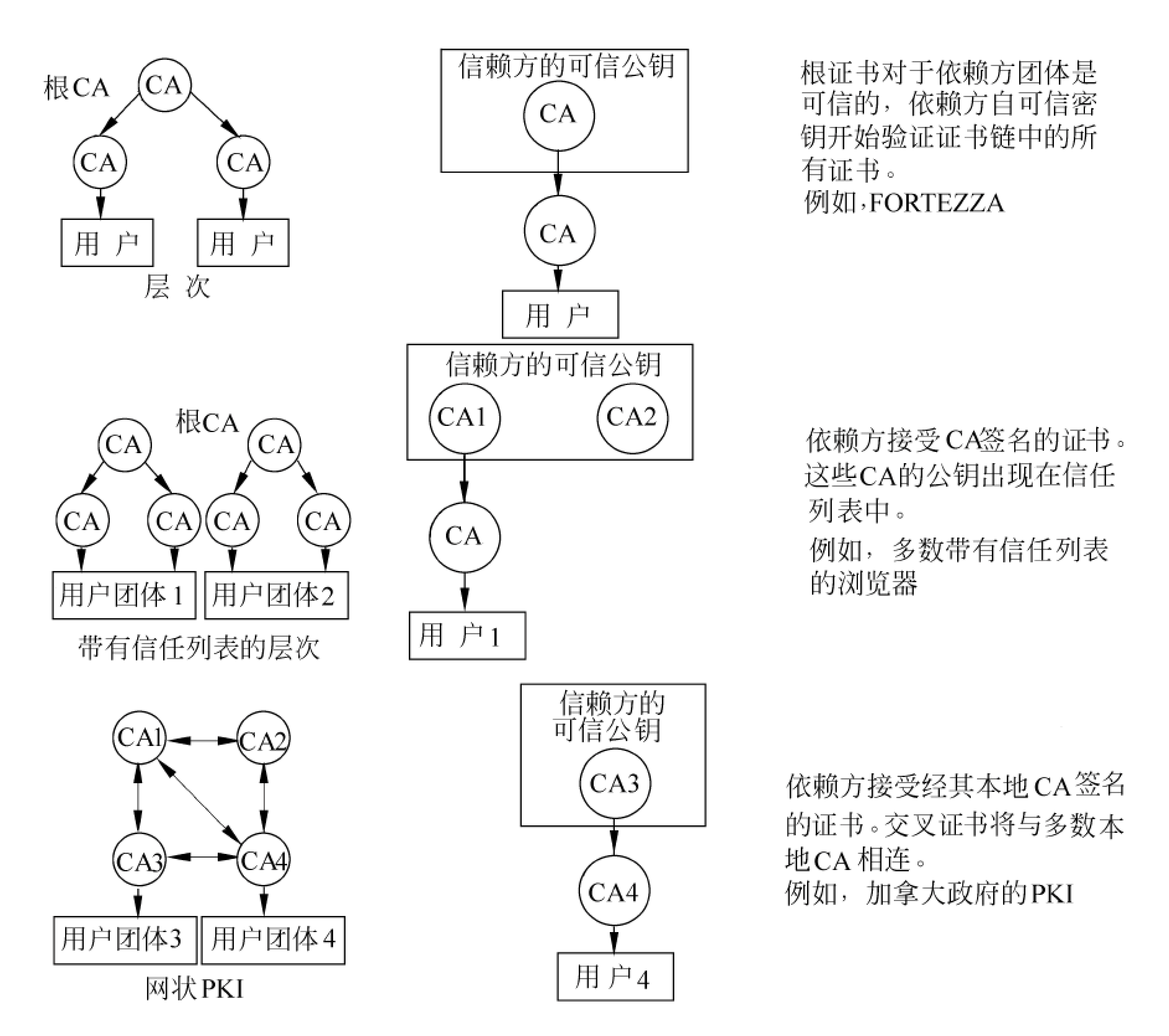


图 18-3　PKI 互操作中的分层信任列表与网状方法

PKI 在密钥和证书的产生、分发和管理中起着关键作用，密钥和证书的产生、分发和管理是实现基于公钥的安全服务所必需的。PKI 本身使用机密性安全服务保护私钥在存储和分发中的安全性，使用完整性安全服务对公钥进行认证，PKI 对公钥的数字签名保证了公钥与证书中的用户身份信息的绑定关系，同时确保了证书中公钥的完整性。

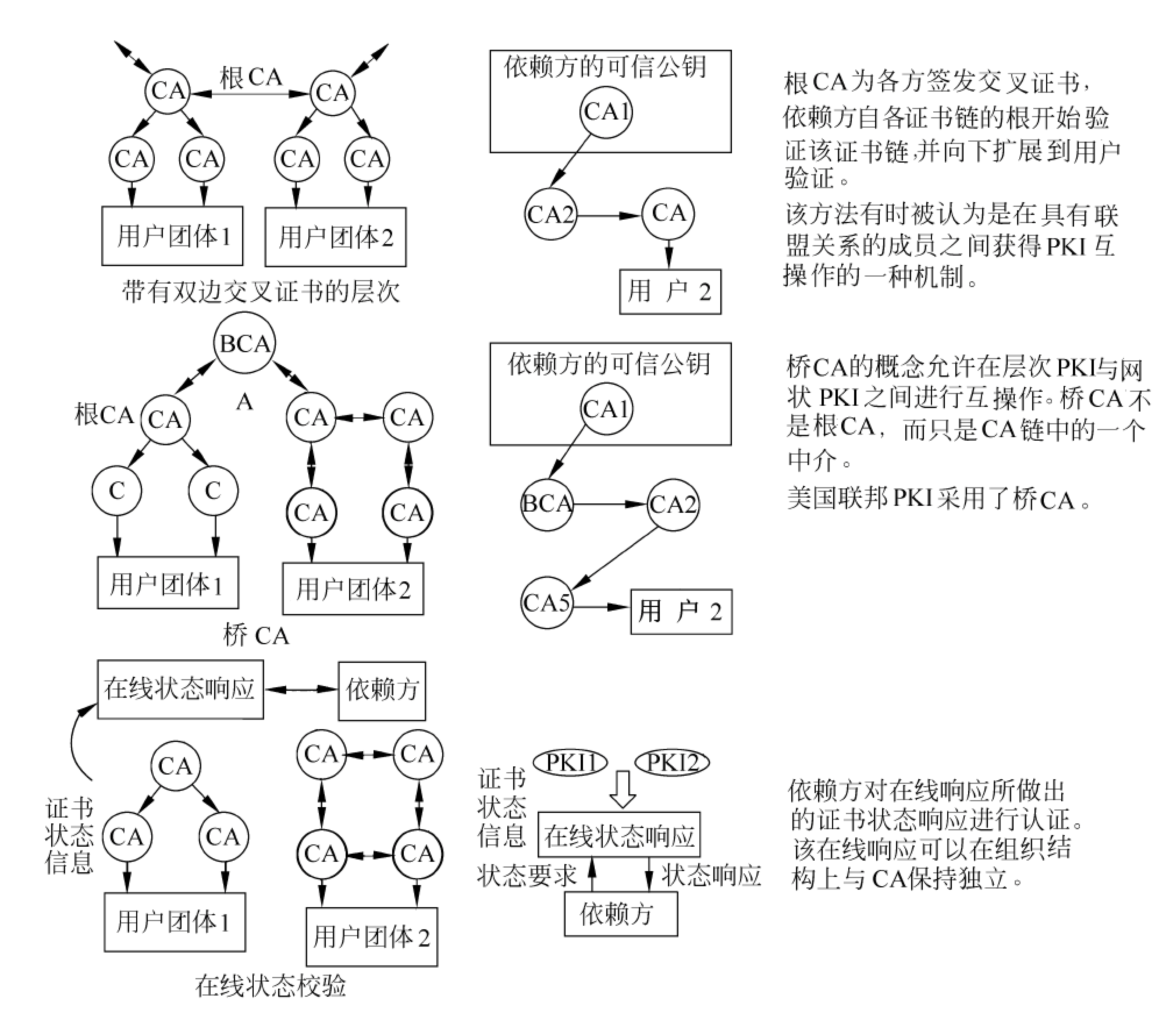


图 18-4　基于双向交叉认证、桥 CA 和在线状态检查互操作模型的 PKI

18.6 对称密钥管理

尽管 PKI 有很多优点，正在得到广泛应用，但在现实世界中，对称密钥管理仍然是一种重要技术。很多现存的系统唯一地使用对称密码。甚至随着非对称密码技术应用的不断发展，许多新出现的应用，例如多点传送，将仍然要求安全的对称密钥和非对称密码系统。

在对称密码算法中，加密密钥可以从解密密钥求得，反之亦然。这一点和公钥密码算法不同，从加密密钥难以计算出解密密钥。在大多数对称密码系统中，加密和解密密钥是相同的，这要求发送者和接收者在相互传送加密报文时约定一个密钥。

如果密钥系统所用的密钥管理很脆弱，密码算法的健壮性就为零。对称密钥应用要求所有用户拥有一个共同的安全密钥，正确安全地分发、管理密钥会十分复杂和昂贵。

18.6.1 对称密钥管理的关键因素

对称密钥管理的许多方面对于维护安全都是至关重要的。对称密钥的管理涉及整个的密钥存活期，必须建立密钥定购、产生、分配、存储、记录、销毁的可控过程，图 18-5 是对称密钥管理活动的关键因素。必须有检测受到篡改的密钥以及使系统恢复安全的方法和

规定，并能有效地确定受到的危害程度。

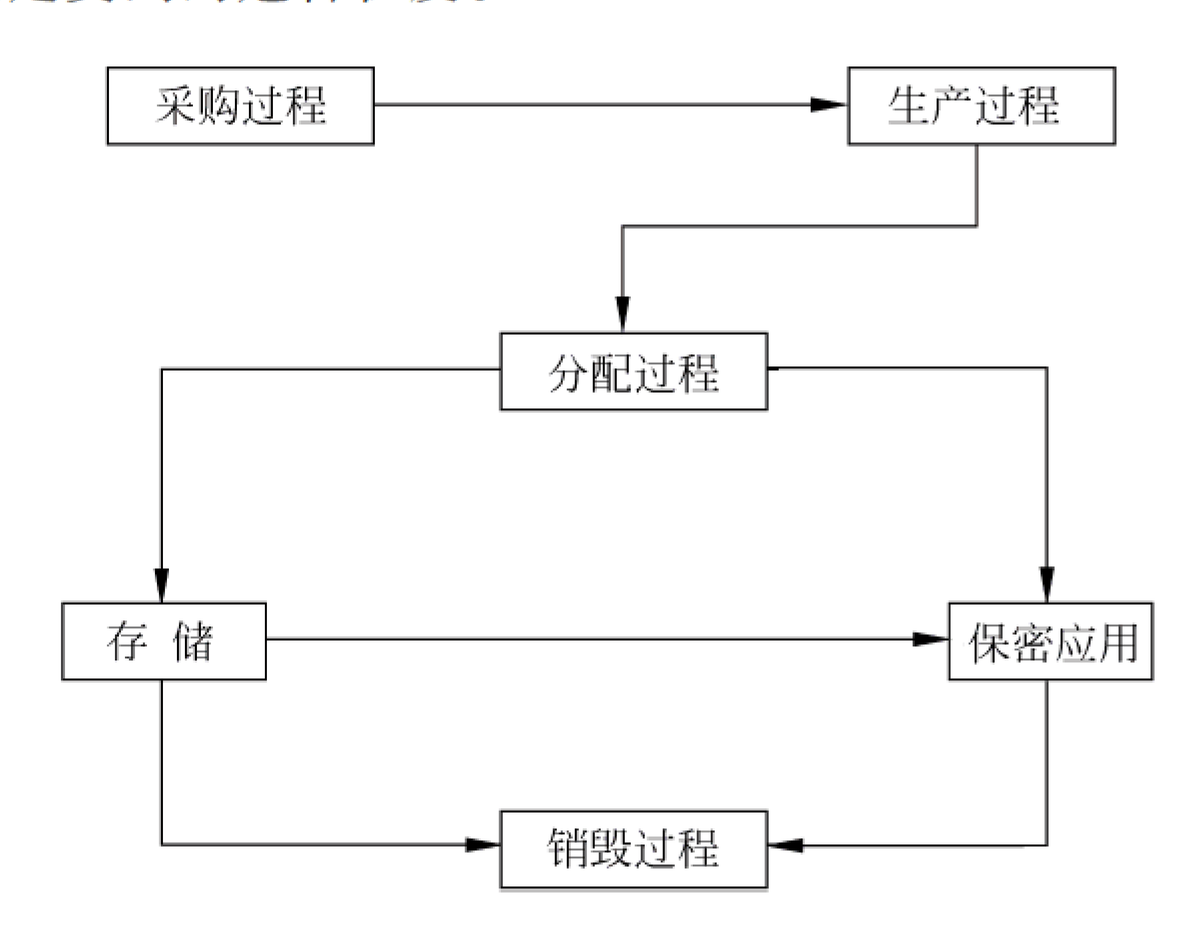


图 18-5　对称密钥管理活动的关键因素

① 定购。只有授权的个体才允许定购密钥，只有得到明确授权的密钥才可以定购。定购者必须具有对通信网络管理的访问权限，定购密钥是为了在需要密钥之前将密钥分发给所有的用户。密钥管理系统将保证定购者具有定购密钥的权限以及接收者具有接收密钥的权限。

② 产生。必须在安全环境中产生密钥以防止对密钥的非授权访问。对于特定的加密算法，产生过程将能产生一组可公认的密钥。对称密钥通常是随机的比特流，因此需要一个性质控制过程保证比特流的随机性。

③ 分配。对称密钥可以通过可信的人或一些保护技术（如抗窜扰装置），以物理形式进行分发。对一些非常敏感的密钥，可以使用两人控制来得到更多的保障。然而，这些技术只能在密钥的存活期提供最小的保护。可以访问密钥的人越多，篡改的可能性就越大。因此，安全分配的目标是通过良好的分发技术将密钥从产生器通过电子手段传送到用户设备。公钥技术可以支持良好的分发技术，允许用户设备产生一个授权的会话密钥，由产生器传送对称密钥。

④ 存储。密钥在等待分发给用户或偶然使用时，必须存储起来。当一个连接失败时，需要有一种机制来保证恢复未经加密的对称密钥的存储区。对这些密钥的保护十分关键，必须安全地存储。以物理形式分发的密钥只能通过严格的物理和人员安全性进行保护。电子形式的密钥应以加密的形式进行存储，同时应采取物理的、人员的和计算机的安全机制来限制对密钥的加密和访问。

⑤ 保密应用。在密码系统的应用中注入密码需要一个保护接口，在接口处对密钥进行物理保护，对于防止密钥的篡改十分关键，因为可以在接口处对密钥进行复制和替换。尽管注入加密密钥只需要最少的保护，但对于相应的解密密钥却需要非常高的保护来限制它注入的频度。

⑥ 销毁。可以有多种可能的介质存放对称密钥，包括纸（例如手工代码本、密钥带）和电子器件（例如随机访问存储器（RAM）、电子可擦写可编程只读存储器（EEPROM）、可编程只读存储器（PROM））。由于对称密钥篡改具有能够恢复以前加密的通信流的特性，所以密钥的存储期不能长于必需的任务执行期是十分必要的。在密钥周期结束后，安

全的密钥必须在所有位置进行销毁，包括偶然存储及伴随的电子存储等。

⑦ 篡改。对称密钥易受到密钥篡改的攻击（例如物理分发、大规模加密网、长加密周期），因此密钥篡改的检测和恢复是十分关键的。目前尚无完善的机制来控制密钥篡改对网络造成的危害。安全密钥的篡改可能会暴露所有它加密的通信流，使假定的对于未来通信流的认证失效。为了恢复密钥的篡改，需要通知每一个用户并提供新的密钥。但对于大规模的加密网，这种方法很难做到使用户同时得到通知和替换密钥。

⑧ 审计。必须采取附加的机制来跟踪密钥的整个存活期。有效的审计可以改进对于密钥的跟踪，如谁得到授权访问密钥、密钥在什么时间分发到什么地方、密钥什么时候销毁。

18.6.2　对称密钥技术的优缺点

1. 对称密钥技术的优点

- 通信网络中的每一个人可以尽可能长久地使用一个密钥，在安全策略允许的情况下，可以经常或很少改变密钥；
- 密钥在本地产生可以使采购的分发的问题最小化，不需要和中心权威机构通信；
- 对称密钥的结构相当简单，主要是一系列随机数；
- 对称密钥处理通常比非对称密钥处理要快得多，在很多情况下，非对称密钥用于在网络中安全地向其他用户分发对称密钥；
- 支持网状的点对点的操作；
- 对称密钥限制对特殊密钥的拥有权，因而，不需要额外的访问控制机制来控制谁和谁通信；
- 对称密钥在使用前不需要广泛地确认；
- 在采购和分发路径中需要信任的人更少；
- 非授权密钥的产生只有当攻击者使某人替代正确密钥使用时才是危险的，它自身是没有危害的。

2. 对称密钥技术的问题

- 一个丢失的密钥将会危及全网的安全，从而要求更换每一个用户的密钥；
- 提供有限的密码服务（例如没有抗否认、隐含认证等）；
- 对于使用共同密钥的密码系统的网络规模有一个上限，很难扩展到大的团体；
- 使用共同的对称密钥的操作员人数越多，密钥篡改的危险就越大；
- 为了对付可能的危害和偶然的使用，需要产生大量的对称密钥，这些密钥必须被安全地传送和在本地存储；
- 分配延迟使得密钥在使用之前就要产生并分发出去，所以在延迟时间较长时，会允许对于密钥的有害访问；
- 网络必须是预先确定的，很难产生动态的通信网络；
- 密钥必须在所有时间保密；
- 对于每一次会话通信，密钥的存活期不能太长；
- 没有固定的方式能够知道谁产生了密钥；
- 没有后向的通信业务保护，从密钥周期的开始，任何时间密钥受到的危害都会使使用该密钥加密的通信业务暴露。

18.7 基础设施目录服务

基础设施目录服务是通过一个结构化的命名服务，提供在分布环境中定位和管理资源的能力。目录也提供对这一分布信息服务中所表示的所有客体的访问控制。目录的设计可以根据客体的内容范围和服务范围进行分类。图 18-6 是目录服务模型，它提供对称及非对称密钥以及整个企业的保密性、完整性、标识和鉴别的管理数据。

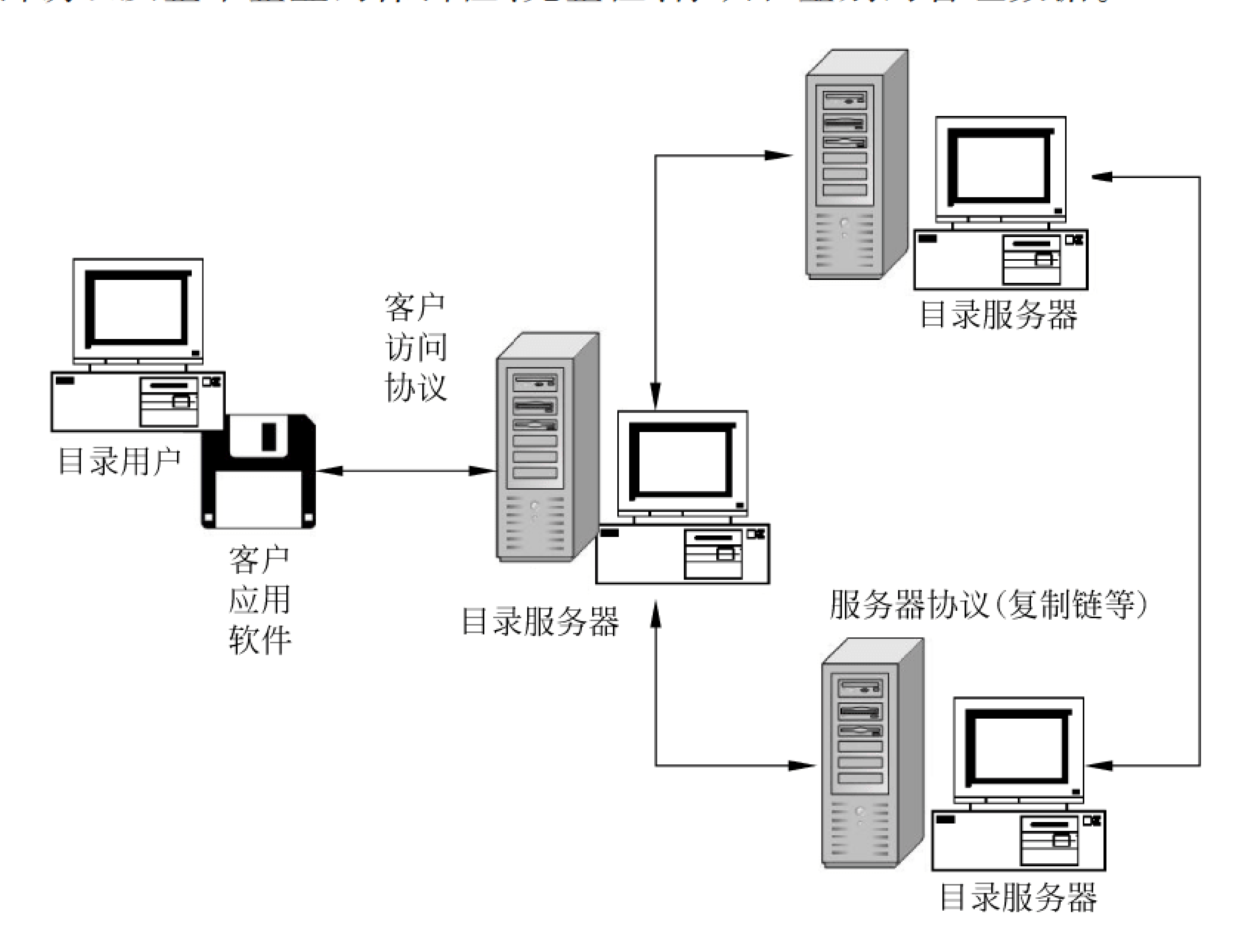


图 18-6　目录服务模型

基础设施目录服务提供了信息的多个元素与特殊的人与设备相关联的方式。这一关联在分层组织中进行管理，并由名字关联进行索引。最常见的例子是电话簿支持地址和电话号码的名字解析关联。在分布式网络环境中，需要管理更多的信息，要求更通用的目录功能。

18.7.1 基础设施目录服务的特性

基础设施目录服务具有以下几个重要特性：

- 定义的名字空间。目录服务通常调用一分层的名字空间，它在逻辑结构上是一棵倒转的树。这一命名格式可用于加强访问和减少用户的位置信息。可以使用 X.500的可辨别名、RFC 822 电子邮件的命名和 DNS 的域名。
- 高度的分布性。目录服务将数据可靠地分布于多个目录，不管它们分布于整个企业还是位于一个局域环境中。提供了允许信息分割以及访问约束和适时的访问机制。此外，通过目录服务复制数据的能力使系统能更好地抗失效和保持可访问性。
- 优化的数据恢复。目录服务提供了根据客体的个体属性进行搜索的能力。该设

计支持很高的读写运算比。大多数目录产品假定访问目录信息库中 99%是查找或搜索，而没有改变、添加、删除。

基础设施目录服务能提供对多种应用的访问。一些重要的访问目录应用如 X.500 目录访问协议 DAP 和 LDAP、电子邮件(S/MIMI V3)和以 Web 为基础的访问(http)。

访问目录服务的客户类型有 3 类：

(1) 查询客户，执行对用户信息的一般查询。

(2) 修改客户，执行查询，并且能执行很强的认证绑定和对选定用户属性的修改。

(3) 管理用户，除了具有修改客户所有的重要特性外，还允许管理用户项和操作信息。

图 18-7 从目录用户和管理者的角度描述了目录信息库(Directory Information Base，DIB)的逻辑结构。目录服务定义了客体、属性和相关句法的关系。用户信息部分包括关于目录客体的信息，这些信息对 DIB 的访问是可见的。DIB 的操作和管理部分包括用于跟踪目录操作的信息元素，如访问控制信息与数据复制的有关信息。

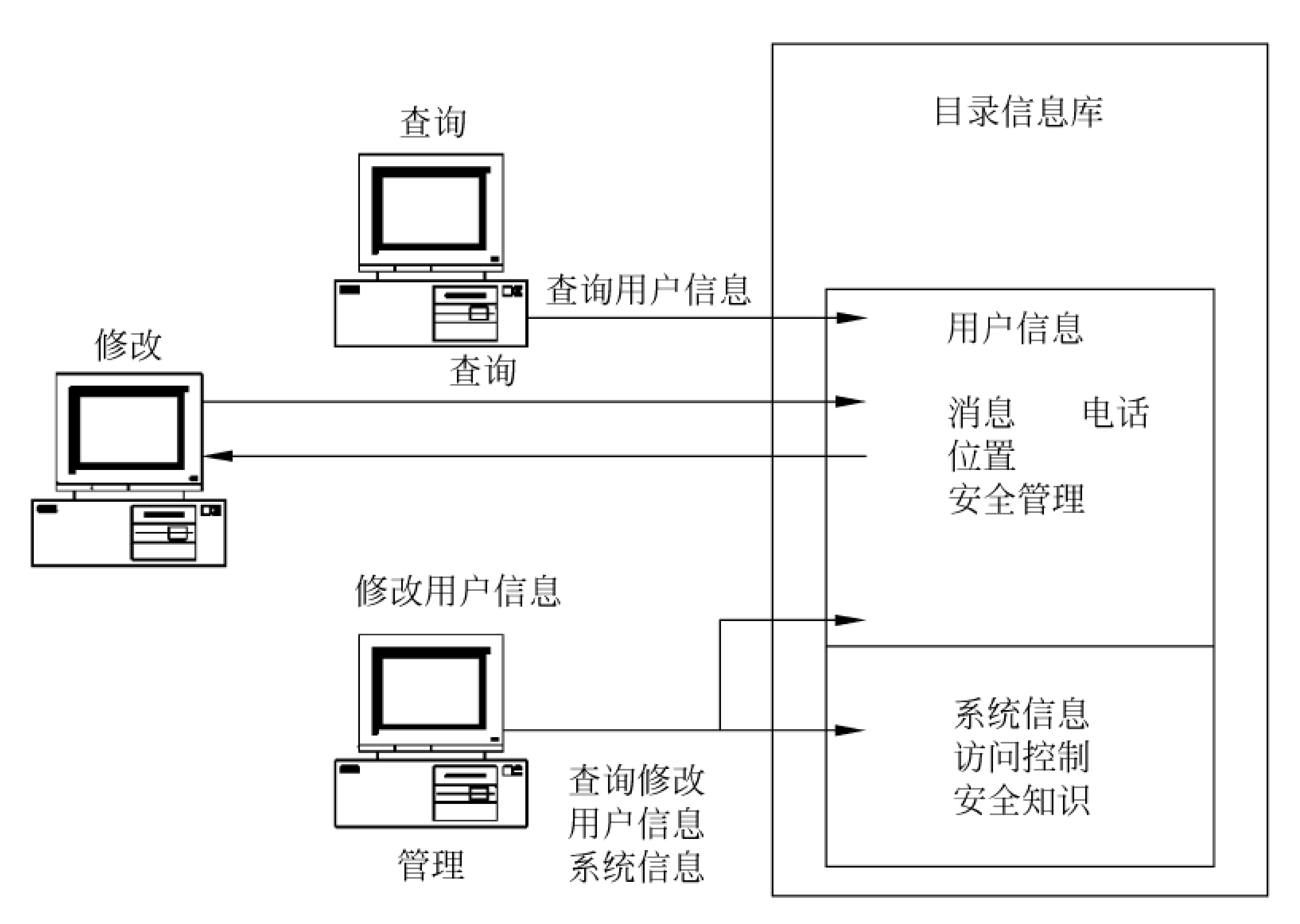


图 18-7　目录信息库的逻辑结构

目录系统是一组定义了目录信息树(Directory Information Tree，DIT)如何构造的规则集合，定义了 DIB 中保存的特定信息类型以及用于访问信息的句法。目录系统由 3 部分组成：

(1) 类，所包含客体的集合。

(2) 每一客体类的属性，某类客体所允许的属性集合。

(3) 属性句法，描绘了句法形式和那一属性使用的匹配规则。

18.7.2　目录服务的实现考虑

目录服务必须具有实际的性能特性，性能可从以下几方面考虑：易用性、健壮性、服务恢复的及时性和响应速度。

易用性是指系统设计和提供给目录用户的工具能方便使用，如单击、指向、图标、窗

口、脚本和状态信息等。

健壮性指产品和系统的可靠性和完整性，并根据平均失效时间 MTBF 和平均修复时间 MTTR 来说明。

可用性目标是提供任何目录服务要 1 周 7 天、1 天 24 小时的可用。在证书管理中，在需要时，吊销信息的操作必须可用。

服务的恢复涉及单个的目录存储代理（Directory Storage Agent，DSA）为达到某一操作状态从客户（和别的附属 DSA）到另一 DSA 之间转换的恢复时间。如果 DSA 在战略环境中，不应超过 5 分钟，在战术环境中应小于 1 分钟。

对于响应速度的战术要求，目录系统提供两种类型的访问特性。一种是人的访问要求，通过人机接口处理信息的获取（例如白页信息）。另一种是通过特定的系统函数（例如在报文转送时，需要名字到地址的解析功能），这一接口是机器至机器的接口。上述两种访问都有性能要求，但是，它们的特征和表示方法却差别很大。

18.8　信息系统安全工程

信息系统安全工程（Information System Security Engineering，ISSE）的含义是为实现客户信息保护需求而进行的某种过程。ISSE 是由美国国家安全局发布的《信息保障技术框架（IATF）》3.0 版本中提出的设计和实施信息系统安全工程方法。图 18-8 表明系统工程过程的主要行为，也反映了进程中各行为之间的关系。箭头表明各行为间的信息流向，而不是行为的顺序或时限。“有效性评估”对各行为的产物（产品）进行评估，使之在指定的环境中依照质量需求标准执行功能需求并以此确保系统能够满足用户需求。

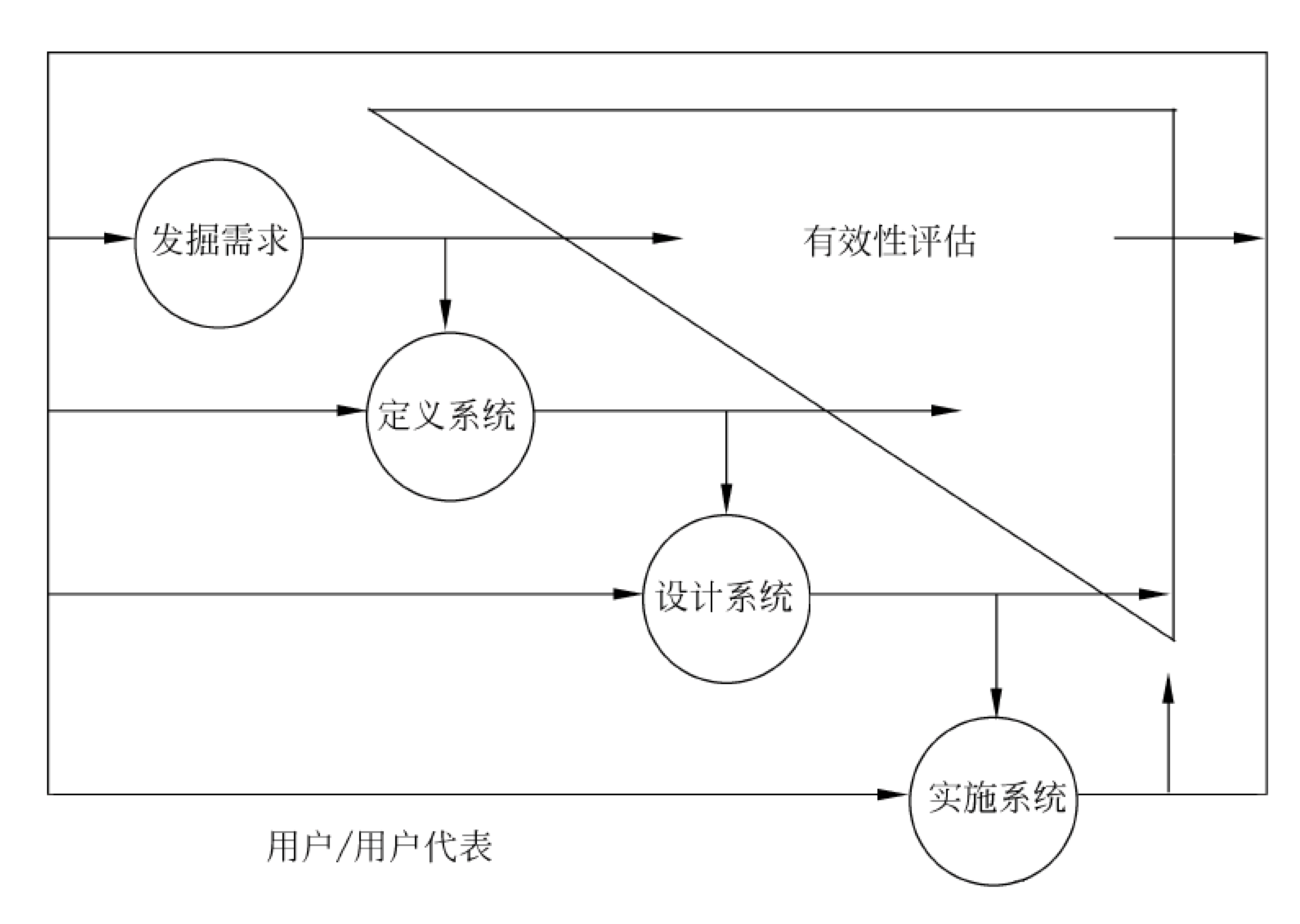


图 18-8　系统工程过程

图 18-8 所描述的系统工程行为的流程是按照下述一般方式进行的：挖掘任务或业务需求，定义系统功能，设计系统，实施系统，有效性评估。该系统工程的过程执行原则是：从“解决方案空间”中分离出“问题的空间”。问题空间表示“解决方案”这一概念的约

束条件、风险、策略和一些界限(值)。解决方案空间代表了在开发系统以满足用户需求时所有已结束的行为和创造出的产品。由解决方案空间所代表的、面向已定义的或一致的目标的系统工程行为和产品在开发的过程中必须不断地接受有效性评估,并确定该方案是否违背问题空间所形成的条件。这些评估是对问题空间和解决方案空间进行必要修正的基础。从解决方案空间分离出问题空间这一原则允许创造并且定义与既成的法律和人为制定的政策保持一致的有效解决方案。

ISSE 支持系统产品的开发—生产—销售全过程的进展、验证和确认,以便满足用户的信息保护需求。同时,ISSE 也识别和接受信息保护风险并对其进行优化。ISSE 行为主要用于以下情况:描述信息保护需求;根据系统工程的前期需要产生信息保护的具体需求;在一个可以接受的信息保护风险下满足信息保护需求;根据需求,构建一个此信息保护需求的逻辑结构;根据物理结构和逻辑结构分派信息保护的具体功能;设计系统用于实现信息保护的结构;从整个系统的耗费、规划和执行效率综合考虑,在信息保护风险与其他 ISSE 问题之间进行权衡;参与涉及其他信息保护和系统学科的综合研究;将 ISSE 过程与系统工程和获取过程相结合;以验证信息保护设计方案并确认信息保护的需求为目的,对系统进行测试;根据用户需要对整个过程进行扩充和裁减,以此支持用户使用。

为确保信息保护被纳入整个系统,必须在最开始进行系统工程设计时便考虑 ISSE。另外,要针对具体的情况,综合考虑信息保护的目标、需求、功用、结构、设计、测试和实际应用中所出现的系统工程设计情况。

18.8.1　发掘信息保护需求

系统工程过程运作的起点是针对用户需求、相关策略、规则和用户环境标准的一系列决定。系统工程师要识别所有的用户及其与系统交互的本质,识别他们所扮演的角色、承担的责任以及在该系统生命周期各阶段中的授权。需求由用户产生,并且不应该对系统设计与执行产生过度的约束。获得文档是过程中的一个必要步骤。该文档通过用户语言来描述工程任务或期望的性能、工程现有性能缺陷与市场机遇、(市场)环境以及如何利用系统达到任务目标和获得市场定位。

ISSE 首先调查用户需求、相关政策、规则、标准以及系统工程所定义的用户环境中的信息所面临的威胁。然后,ISSE 识别信息系统中的具体用户和信息,以及他们在信息系统中的相互关系、规则及其在信息保护生命周期各阶段所承担的责任。信息保护应当允许用户有自己的观点,不能局限于特定的设计或者应用。

在信息保护政策和安全操作概念中,ISSE 应该使用通用语言描述如何在一个综合的信息环境中获得所需要的信息安全保护。当系统发现需要这种信息安全保护时,信息保护将成为一个必须同时考虑的系统模块。图 18-9 解释了系统任务、威胁和政策如何影响信息保护需求以及如何进行分析。

1. 任务的信息保护需求

我们必须考虑信息和信息系统在一个大型任务或特定组织中的作用。ISSE 必须考虑组织元素(人和子系统)的任务可能受到的影响,即无法使用所依赖的信息系统或信息,

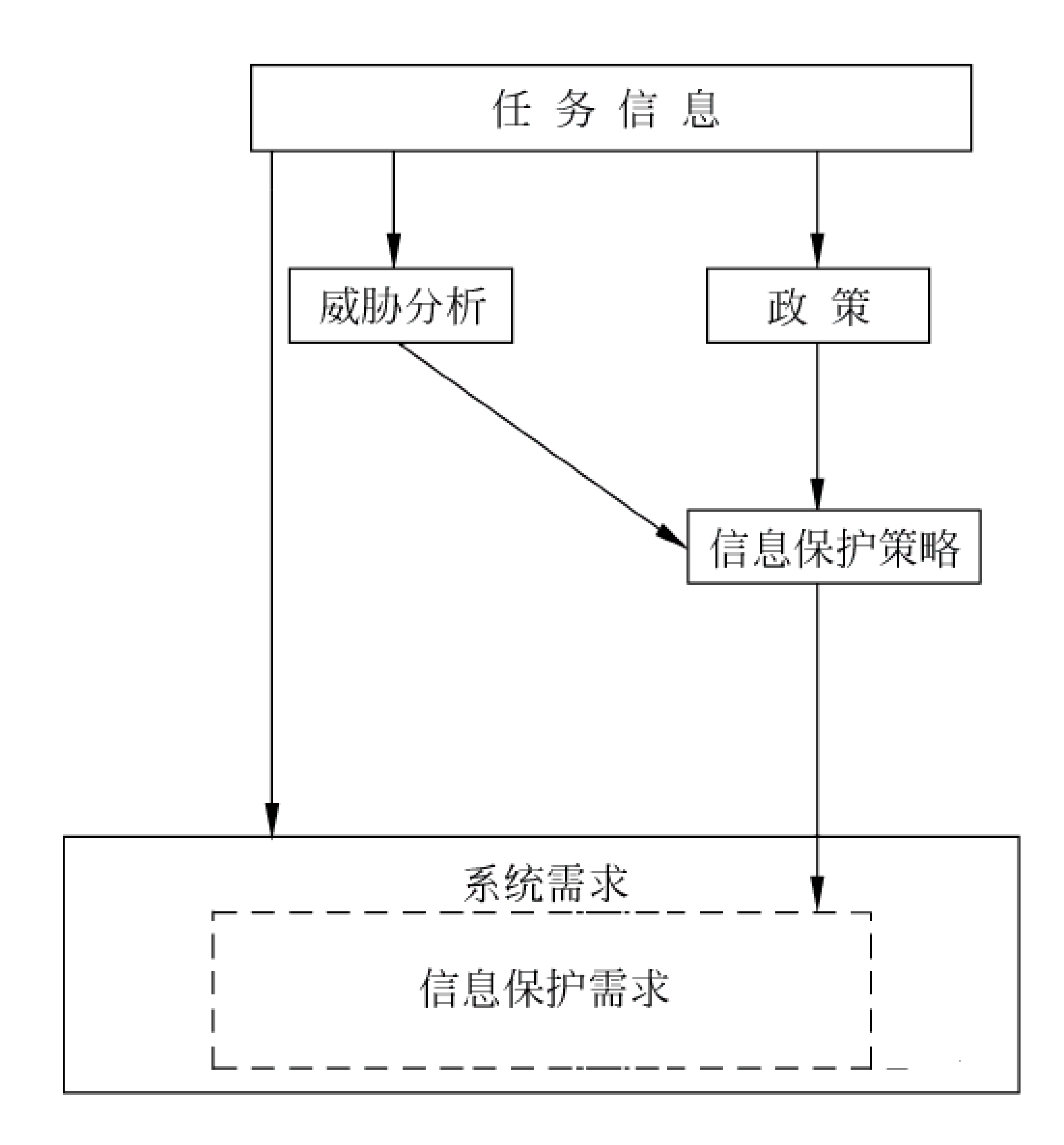


图 18-9　系统任务、信息安全威胁和政策对确定信息保护需求的影响

尤其是丧失机密性、完整性、可用性、不可否认性及其组合。在此意义上，ISSE 已经开始探讨用户信息保护需求问题。

信息的重要性众人皆知，但是人们往往忽视信息保护需求。要发现用户信息保护需求，必须了解遗漏、丢失或修改什么信息会对总体任务造成危害。ISSE 应该做到以下几点：帮助用户对自己的信息管理过程进行建模、帮助用户定义信息威胁、帮助用户确立信息保护需求的优先次序、准备信息保护策略、获得用户许可。

ISSE 提供了识别顾客需求的界面，以确保任务需求包含信息保护需求，并且保证系统功能包含信息保护功能。ISSE 将安全规则、技术、机制相结合，并将其应用于解决用户信息保护的实践需求，从而建立一个信息保护系统。该系统包含信息保护体系结构和机制，并能够依据用户所允许的耗费、功能和计划获得最佳的信息保护性能。

图 18-10 描述了一个分层的结构，较高层次的需求建议在较低层次的需求基础之上，各模块的需求决定于它在结构图中的位置。

ISSE 在设计信息系统时必须遵循用户的层次设置，这样才能使整个系统的性能达到预期指标。信息和信息系统在支持任务方面必须满足如下要求：对何种信息记录(机密信息、金融信息、产权信息、个人隐私信息等)进行观察、更新、删除、初始化或者处理？授权谁观察、更新、删除、初始化和处理信息记录？经授权的用户如何履行其责任？经授权的用户使用何种工具(文档、硬件、软件、固件和规程)履行其责任？清楚地知道个人发送或者接收的一则消息或一个文件具有怎样的重要性？

ISSE 和系统用户将精诚合作，使信息系统更好地满足用户总任务要求。没有用户的参与，ISSE 很难做出满足用户要求的决定。

2 信息管理面临的威胁

依照 ISSE，技术层面的系统组成应负责识别信息系统的功能和它与外界系统边界的

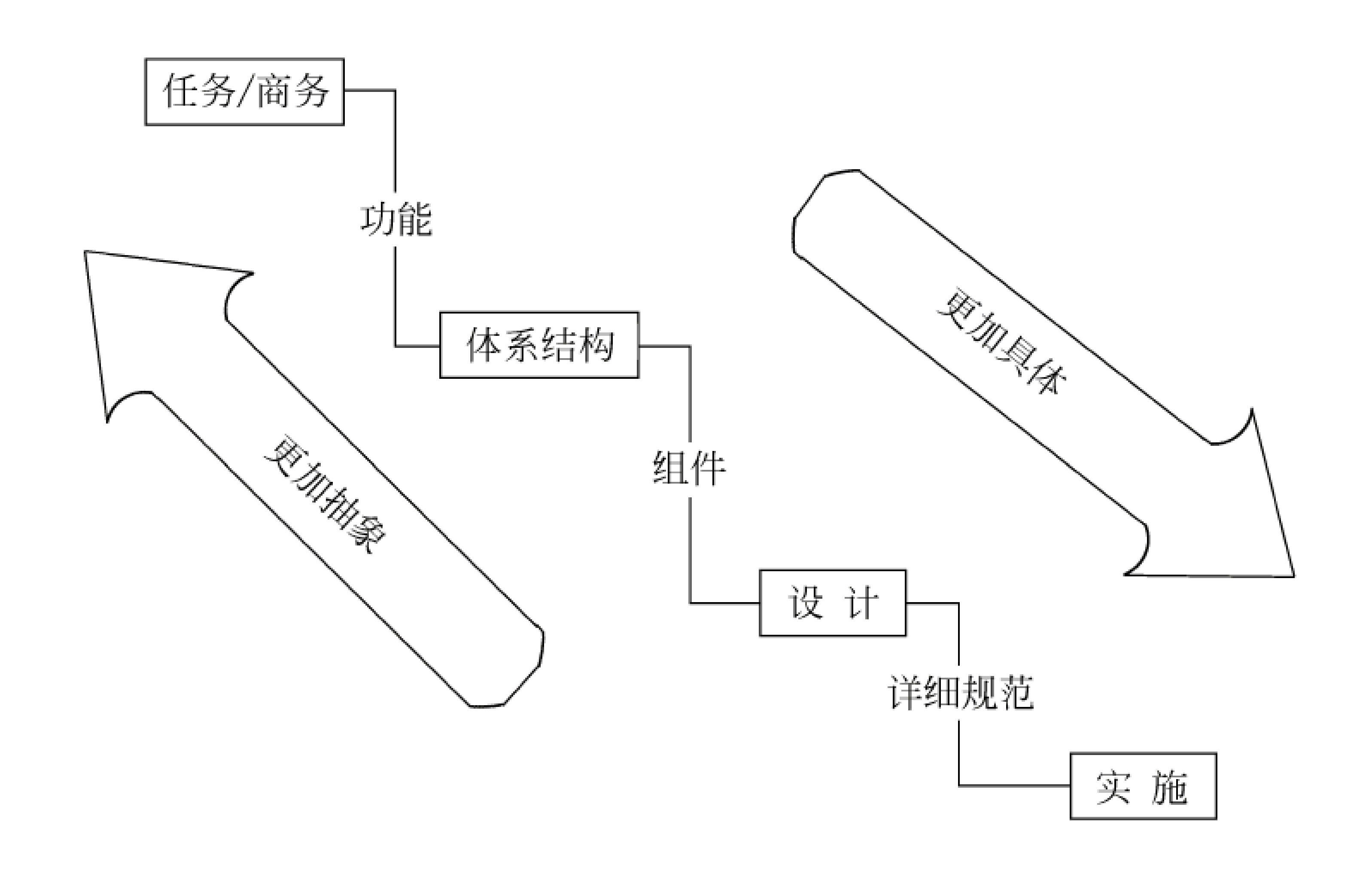


图 18-10　分层需求图

接口。该系统组成要明确信息系统的物理边界和逻辑边界，以及系统输入输出的一般特性。它描述系统与环境之间或系统与系统之间信号、能量和物质的双向信息流。必须考虑系统与环境之间或系统与系统之间信号、能量和物质的双向信息流。必须考虑系统与环境之间或系统与系统之间有意设定或自行存在的接口。其中，针对后者的部分描述涉及环境和信息系统所面临的“威胁”。“威胁”指某些人采取某种行动，引发可能造成某个结果的事件或对系统造成危害的潜在事实。对系统威胁的描述涉及信息类型、合法用户和用户信息、威胁者的考虑（能力、意图、自发性、动机、对任务的破坏）。

3. 信息保护策略的考虑

对一个机构而言，在制定本组织的信息保护策略时必须考虑所有现有的信息保护策略、规则和标准。必须定义下面的信息保护最重要的内容：为什么需要信息保护？需要什么样的保护？怎样获得保护？

与系统工程过程相同，一个机构必须考虑本机构内所有的政策、规则和标准。必须定义一个机构信息策略的以下最重要内容：机构需要保护的资源/资产、需要和这些资产发生关系的个人的角色和责任（作为可操作性任务的一部分）、授权用户用到这些资产（有信息安全要求）的合适的方法。

为制定一个有效的信息保护策略，需要设立一个由系统工程专家、ISSE、用户代表、权威认证机构、设计专家组成的小组。该小组的成员要共同合作，保证策略的正确性、全面性以及和其他现有策略的连续性。

高层管理机构要颁布信息保护策略。该策略必须是明确的，应该使下级机构易于制定各自的制度，并且便于机构所有成员的理解。需要一个能够确保在机构内部实施该策略的流程，并让机构成员认识到，如果不实施该策略将会出现怎样的后果。尽管必须依据具体情况的改变及时更新机构安全策略，高层策略却不应经常变动。

18.8.2　定义系统功能

1. 目标

在系统开发的系统功能定义阶段，系统工程师必须明确系统要完成的功能，该功能的实现应达到什么程度，以及系统有哪些外部接口。系统工程也要将描述系统应用环境的自然语言翻译为定义接口以及系统边界的工程图表。

需求到目标、目标到要求以及要求到功能的各翻译环节均采用工程语言。系统工程师将使用工程语言来描述特定的目标。目标描述能够通过描述系统的预期运行效果而满足需求。系统工程师必须能将目标同此前提出的需要相联系，并且能够从理论上加以解释。各目标都有一个描述满足该目标所需条件的有效性量度(MoE)。因此目标描述必须明确、可测、可验证。当所有的需求目标得以实现时，如果先前从需求到目标的解释正确而且完整，这些需求便得以满足。

信息保护目标与系统目标具有相同的特性，都具有 MoE，而且对信息保护需求是明确的、可测量的、可验证的、可跟踪的。每个目标的基本原理必须解释为：信息保护对象所支持的任务目标、驱动信息保护目标的与任务相关的威胁、未实现的目标的结果、支持目标的信息保护指导或策略。

2 系统描述/环境

技术系统描述本系统与系统边界外的元素相互作用的功能与接口。系统描述应当包括系统的物理边界和逻辑边界，以及系统输入输出的一般特性。系统描述包括针对信息、信号、能量和资源在系统与环境之间或系统与系统之间双向流动的描述。系统描述应当指出为完成用户任务所需的信息处理类型(例如对等通信、广播通信、信息存储、一般访问、受限访问等)。

3. 要求

功能要求由父目标处继承而来。功能要求描述系统需要完成的任务、动作和行为。当转化为性能需求时，目标有效性度量则定义功能需求的实现程度。除了规定系统的功能、接口、性能、互操作性、继承以及设计需求外，系统工程师也必须与用户共同决定系统开发和升级的保障要求。保障要求影响系统设计与文件归档方法，并使用户确信系统除了实现开发者声称的功能之外再无其他功能。这里的保障可以特指系统的性能要求，也可以特指某种验证并确认系统可靠方法的处理要求(分别对设计和适用性而言)。为确定一套能够满足需求并代表可接受的风险、生命周期成本和进度的性能的要求集，系统工程师在为一套要求或其他要求进行性能分配时必须进行多方面的权衡考虑。性能要求的典型形式如下：质，多好？量，数量？每个系统的成本有多高？适用范围，适用范围有多大？合时性，使用频率与响应度如何？有备性，可靠性、可维护性、可用性、可生产性。

内部接口、外部接口与互操作性要求是可能产生于系统成员之间或系统与环境、系统与系统之间的相互作用概念的重要要求。此外，政策也可能规定某些接口、互操作和设计要求。为实现系统功能，系统工程师可能需要依据这些要求提出其他要求。

当明确所有要求之后，系统工程师必须同其他系统负责人商议评估这些要求的正确

性、完整性、一致性、互依赖性、冲突和可测试性。正确解释目标的要求应既不苛刻也不模糊。极端苛刻的要求是不合适的,它对一些系统性能要求太高,并可能修改其他某些合理要求。所有正确的要求都必不可少,并且它们的集合足以满足用户需求。各种要求必须是一致的。对用户、客户或开发者而言,它们代表同一个特定事物。系统工程师必须解决不同要求之间的冲突,并通过与其他系统责任人进行协商的方式淘汰和修改某些要求。除非政策规定了一定的设计方案,否则要求应当与系统实施保持独立。用户应该区分要求的优先级。在发生冲突的情况下,可以在必要时放弃低优先级的要求,以缩短时间、降低成本、减少风险和缩小范围。尤为重要的一点是,由于需满足的要求是系统有效性和可用性的基础,系统负责人必须在这些要求和要求特性上取得一致意见。

4. 功能分析

功能由要求决定,每个要求产生一项或几项功能。由于对要求和功能的定义不同,初始功能的级别高低并不相同。功能分析的主要内容是分析功能之间或功能与环境之间的联系。

通过图表描述功能的相互联系有多种方法。最简单的图表是文本功能列表。它通过习惯性的缩写、标号、字体来描述一系列功能的层次结构。功能列表对功能进行命名,并且描述其定义、行为、何时被调用、输入输出。开发最简单系统时,系统工程师可能只需功能列表就足够了。但通常情况下,功能列表只是最初级的功能分析。

由于功能列表具有分层的特点,它也可以是一个树型结构。这两种分析的考虑过程要求系统工程师考虑系统集成的相应程度和与该程度对应的功能。将更高层次的功能和继承功能视为一组,使它们与其他功能保持高度的独立性。这是定义一个模块化结构的部分工作,模块化结构具有连带关系(每一个模块或子系统产生一个系统功能,该系统功能由紧密联系的低层功能构成),同时也具有弱耦合结构(各模块或子系统之间在很大程度上保持相互独立)。系统工程师必须在连带和耦合之间进行权衡,模块化系统几乎可以与独立的子系统一样定义、设计、开发、测试、移植和升级。通过权衡可以产生各种可能的系统结构。这样便导致了子系统和底层组件的可视化。这些组件和子系统具有各自的功能。

ISSE 将使用许多系统工程工具来理解功能,并将功能分配给各种信息保护配置项。ISSE 必须了解信息保护子系统如何成为整个系统的一部分,如何支持整个系统。

18.8.3　设计系统

本部分工作要求一个受到多方制约的工作组设计系统的体系结构并制定具体的设计方案。系统工程师对体系结构解决方案进行分类并识别所有类似的可重用方案。在此意义上,系统工程师可以组织一个负责开发具体解决方案的工作组。该工作组选择可用于该方案的产品,采用结合可重用方案或设计新方案的方式设计具体的体系结构解决方案。

为达到应用目标,系统必须依赖其所有组件,这一点非常重要。因此,耗费过多精力对某个组件进行优化只是对精力和资源的一种浪费。但是,性能过低的组件可能会损害系统整体性能。系统设计必须满足包括功能、性能、接口、互操作和设计要求在内的一系

列要求。好的系统设计将确保该系统能够满足客户需求。

1. 功能分配

在这个过程中，系统工程师必须明确在实现其功能时应采取的物理形式。他们可以将一些功能分配给软件、硬件、固件和人。执行系统功能的人一般都采用确定的工作程序与书面步骤，使用特定的可用软件、硬件与固件。当系统功能的执行需要具备一致性时，这一点尤为重要。因此，一些功能可由人和机器共同完成。由于功能被分配给组件，组件必须实现相应的功能和性能要求，并且不超出系统规定的出错率。系统工程师必须明确各种体系概念以及依据概念分配给各组件的功能与要求，并同其他系统负责人对概念和物理上的可行性取得一致意见。

在此意义上，系统工程师可以进行方案验证、集成和制定工作系统，以及要求生效的系统验证、集成和有效性测试。必须记录达到预期效果的可用、验证和集成测试计划并将其与要求和体系结构相联系。系统工程师可以开始针对系统设计分配资金、人员、工具和时间资源，为系统分配测试、细节、生命周期支持。多数系统需要正式的结构管理（CM），结构管理应当作用于体系结构。

2. 初步设计

进行系统初步设计至少应具备两个先决条件：确定并且一致的系统要求；结构管理下确定的体系结构。一旦体系结构确定，系统和设计工程师就必须确定用于描述开发内容的规范。该规范必须是同规定的需求相应的、完整的和确定的。规范的细节级别从系统级到组件级。应当在初步设计评审（Preliminary Design Review，PDR）之前对更高级规范进行制定和评审。PDR 产生用于调查完备性、冲突、兼容性（与接口系统）、可验证性、安全风险、综合风险和可验证等要求的高级规范。初步设计的结果是分配系统基线配置。

3. 详细设计

详细设计产生更低层次的产品规范、具体的工程与接口控制图、原型、具体的测试计划与程序和具体的集成供给支持计划（Integrated Logistics Support Plan，ILSP）。专业工程实践、可靠性、可维护性、可用性、质量、安全性和可生产性均能够提供专家水准的具体信息。这些信息可用于确定资源购买或资源开发的内容与方式。详细设计将产生系统关键设计评审（Critical Design Review，CDR）。评审内容涉及针对完整性、冲突、兼容性（与接口系统）、可验证、安全风险、集成风险和可追踪性等要求的所有配置项的具体规范。

18.8.4　系统实施

系统实施的目的是为所设计的系统开发并集成其全部组件。紧接的下一步工作是对系统进行测试和验证，确定系统是否满足要求。在测试过程中，一些非常底层的设计工作（如小软件模块设计）通常作为系统建造工作的一部分。这个工作也包括调查生产该系统的可能性。

系统实施行为形成一个系统验证调查结论。它为所建立的系统遵循系统设计要求并为满足任务性能需求提供证据。必须考虑涉及所有系统工程主要功能的问题，并且确定

其相互依赖关系或进行权衡。

1. 采办

本阶段的工作必须在开发还是购买满足设计系统细节规范的组件这二者间做出决定。针对解决方案的集成选择和获得，可用产品的基础是所选择的系统设计细节。这些产品是采用购买、租用还是借用的方式，决定于许多已知因素（组件价格、是否容易获得、形式、是否合适、功能等）或未知因素（在特殊系统中的可靠性、组件性能的不足可能对系统性能造成的风险、该组件将来是否可用或可被替代等）。在正式决定开发或购买之前，系统和设计工程师必须慎重权衡两种方式的利弊并进行研究。

2 开发

在本阶段，系统开发方法已经被转化为一个稳定的、可生产的、性能代价比合理的系统设计实践。对信息系统而言，转化包括所有产品级别的软件、硬件或固件。

一旦开发出或购买到组件，系统工程的下一步工作就是组织建立系统。在此之前需要采用相应的系统设计规范对各系统组件进行测试。测试结束便可以开始建立系统。为避免不必要的麻烦，组建系统时应遵循生产商规范。

组建过程的完成将对后续工作产生重大影响。如果系统组建正确，后续工作将能精确反映系统设计和工程工作的正确性。反之，系统将无法按照设计意图运行，无法实现设计和任务目标。

3. 测试

组件开发出来后，必须对组件开发结果进行测试。在定义方案之后，系统和设计工程师要写出测试过程和预期的测试结果。设计工程师要进行单元测试。方案和接口验证将保证所开发的组件能够正确实现其功能。在验证和综合测试过程中，必须对所有接口进行全面测试。

综合测试用于验证较高级的系统性能水平。早期工作应尽可能地规定系统测试所需人员、工具、设备、资金资源，并且进行预算和论证。在预定方案中集成经选择、购买或开发的产品，通过测试与调整获得较高水平的系统功能。集成测试可能导致改变系统组件重新设计。系统功能测试报告用于记录测试成功或失败的结果。集成是为用户提供一个全面的集成与测试，并能够确保相应的设计已经通过验证的系统。

一般地，任务需求所要求开发的系统应该具有唯一性，或者该系统将用于某未知或难以模拟的环境。此时，除非合同中的承诺条款承认实验室环境下的系统性能测试结果，否则必须针对实际系统进行测试。这种情况通常与某个政府机构有关。对于将同一系统部署于某个已知和可模拟环境的情况，在生产和部署之前也应进行仔细测试。效用测试和用户可用性测试不一定完全相同。但是，满足这些要求是获得用户认可并争取到下一份商业订单的基础。

在系统验证、系统集成和系统效用测试之后，尤为重要的是针对系统的安装、操作、维护和支持步骤进行归档。这些步骤以需求、体系结构、设计和针对系统建立之初的配置所进行测试的结果为基础。需要重点指出的是，在安装过程中必须记录异常情况，并且注意这些变化对集成和效用测试以及操作步骤可能产生的影响。此外，也要讨论安装过程中

的变化情况对系统操作、支持与维护可能造成的其他风险。

18.8.5 有效性评估

在评估系统效用时，必须检测两个主要的因素。第一，系统是否达到了任务的需求？第二，系统依照任务组织所期望的方式操作吗？对系统功能和操作来说，可能有些预期要求是绝对不能忽视的。系统功能和操作需求是系统能否被认同所要考虑的主要方面。除这些因素之外，也应该注意可能影响评估结果的如下因素：互操作性，系统能正确地通过外部接口共享信息吗？可用性，对用户可供使用的系统能提高任务成功性吗？训练，用户有资格操作和维护系统需要的指令的程度？人机接口，用户出现错误的时候人机接口能够正确协调吗？费用，建立、更新和维护系统在经济上是否可行？

18.9 本章小结

一个安全基础设施应提供很多组件的协同使用，其体系结构可改进整个的安全特性，而不仅是各个安全组件的特性。安全基础设施的主要组成有 4 部分：网络、平台、物理设施、处理过程。

安全基础设施设计的基本目标是保护企业的资产。保护这些资产的方法是适当地部署各个安全组件于有组织的、协同的安全基础设施中。根据选择的数据等级分类体制，每种数据保护目标应按数据机密性、完整性和可用性来表示和衡量。

安全基础设施设计指南中最重要的是要保证企业安全策略与过程和当前经营业务目标相一致。设计基础设施安全服务以支持设计指南和需求，这些安全服务包括鉴别、授权、账户、物理访问控制和逻辑访问控制，应分别采取适当的安全机制以实现这些安全服务。

KMI/PKI 作为一种支撑性安全基础设施，其本身并不能直接为用户提供安全服务，但是其他安全应用的基础。KMI/PKI 是安全服务所必需的组件，其体系结构依赖于其支持的应用。KMI/PKI 支持 4 种服务：对称密钥的产生和分发、非对称密码技术及与其相关的证书管理、目录服务、基础设施本身的管理。

公钥基础设施(PKI)用来管理密钥和证书。PKI 主要组成包括证书授权(CA)、注册授权(RA)、证书存储库(CR)。PKI 管理的对象有密钥、证书以及证书撤销列表(CRL)。大型公钥基础设施往往包含多个 CA，多数 PKI 中的 CA 是按层次结构组成的。桥 CA 的作用是为多个 PKI 中的关键 CA 签发交叉认证证书。

在现实世界中，对称密钥管理技术仍然是一种广泛应用的重要技术。密钥管理是对称密钥技术安全性的关键因素。对称密钥的管理涉及整个的密钥存活期，必须建立密钥的定购、产生、分配、存储、记录、销毁的可控过程。

基础设施目录服务是通过一个结构化的命名服务，提供在分布环境中定位和管理资源的能力。基础设施目录服务的重要特性包括定义的名字空间、高度的分布性、优化的数据恢复以及提供对多种应用的访问。

信息系统安全工程(ISSE)是为实现客户信息保护需求而进行的某种过程。ISSE 是由美国国家安全局发布的《信息保障技术框架(IATF)》3.0 版本中提出的设计和实施信息系统安全工程方法。ISSE 的系统工程过程包括挖掘任务或业务需求、定义系统功能、设计系统、实施系统以及有效性评估。

习　题

1. 安全设计是(　),一个安全基础设施应提供很多安全组件的(　)使用。
   A. 一门艺术,各种　　B. 一门科学,协同
   C. 一项工程,分别　　D. 艺术、科学和工程集成于一体,协同
2. 安全基础设施的主要组成是(　)。
   A. 网络和平台　　B. 平台和物理设施
   C. 物理设施和处理过程　　D. 上面 3 项都是
3. 安全基础设施设计的基本目标是保护(　)。
   A. 企业的网络　　B. 企业的资产
   C. 企业的平台　　D. 企业的知识财产
4. 安全基础设施设计指南应包括(　)。
   A. 保证企业安全策略和过程和当前经营业务目标一致
   B. 开发一个计算机事故响应组 CIRT
   C. 设计基础设施安全服务
   D. 以上 3 项都是
5. 支撑性基础设施是能提供安全服务的一套相互关联的活动与基础设施,最重要的支撑性基础设施是(　)。
   A. KMI/PKI　　B. PKI 以及检测与响应
   C. KMI/PKI 以及检测与响应　　D. 以上 3 项都不是
6. KMI/PKI 支持的服务不包括(　)。
   A. 非对称密钥技术及证书管理　　B. 对称密钥的产生和分发
   C. 访问控制服务　　D. 目录服务
7. PKI 的主要组成不包括(　)。
   A. 证书授权 CA　　B. SSL
   C. 注册授权 RA　　D. 证书存储库 CR
8. PKI 管理对象不包括(　)。
   A. ID 和口令　　B. 证书
   C. 密钥　　D. 证书撤销列表
9. 下列基础设施目录服务的特性(　)是不正确的。
   A. 优化的数据恢复　　B. 定义的名字空间
   C. 高度的集中性　　D. 提供对多种应用的访问
10. 信息系统安全工程 ISSE 是由美国国家安全局发布的《信息保障技术框架

(IATF)》3.0 版本中提出的设计和实施信息系统(　)。

A. 安全工程方法　　B. 安全工程框架

C. 安全工程体系结构　　D. 安全工程标准

第19章 网络安全管理

本章要点:

- 网络安全管理背景——典型的网络环境;
- 网络安全管理过程及其步骤,包括评审整体信息安全策略、评审网络体系结构和应用、识别网络连接类型、识别网络特性和信任关系、识别控制区域、实施和运行安全控制措施、监视和评审实施。

19.1 网络安全管理背景

政府机构和商业组织的信息系统绝大多数都是通过网络连接着的,并且遍及全球的现代网络应用(例如电子政务和电子商务)一直在不断增长。这些网络连接可能在组织内部、不同组织之间或组织与公众之间。

公众可用的网络技术的迅猛发展,特别是互联网和建立在其上的Web,的确为商业和在线公共服务带来了极大的机会。但同时,也带来了新的安全风险。当一个组织极大地依赖于信息与网络进行业务活动时,信息的保密性、完整性、可用性、不可否认性、可核查性、真实性和可靠性的丧失或网络服务的中断可能对业务运行造成不可忽视的负面影响。因此,保护好信息和网络,管理好组织内信息系统的安全是一项迫切的关键要求。

图19-1示出了一个在许多组织中都能看到的典型网络构造场景,包括内联网(Intranet)、外联网(Extranet)、互联网(Internet)、电话网(Phone Network)、无线网(Wireless Network)和非军事化区(Demilitarized Zone,DMZ)。

内联网是一个组织在其内部使用和维护的网络。由于内联网位于组织的场所之内,而且一般只有组织的内部工作人员才能在物理上访问到内联网,所以比较容易对内联网进行物理保护。在多数情况下,由于采用的技术不同及各组成部分的安全要求不同,内联网不是同构的。一方面,有些关键基础设施,例如PKI(Public Key Infrastructure),需要比内联网自身更高保护级别,因此可能放在内联网的一个专门网段中来运行。另一方面,某些技术如WLAN(Wireless Local Area Network),会引入新的风险,因此需要进行某种隔离。对于这两种情况,均可采用内部安全网关来实现上述分割。

当今多数组织的业务都需要与外部合作伙伴或其他组织进行通信和数据交换。对于最重要的业务合作伙伴,通常将内联网直接扩展到对方组织的网络,这种扩展一般被称为外联网。在绝大多数情况下,对所连接的外部合作伙伴的信任度低于组织内部,因此需要使用外联网安全网关来降低这种连接带来的风险。

如今公共网络(主要指互联网)被用来在组织与合作伙伴和客户(包括公众)之间提供

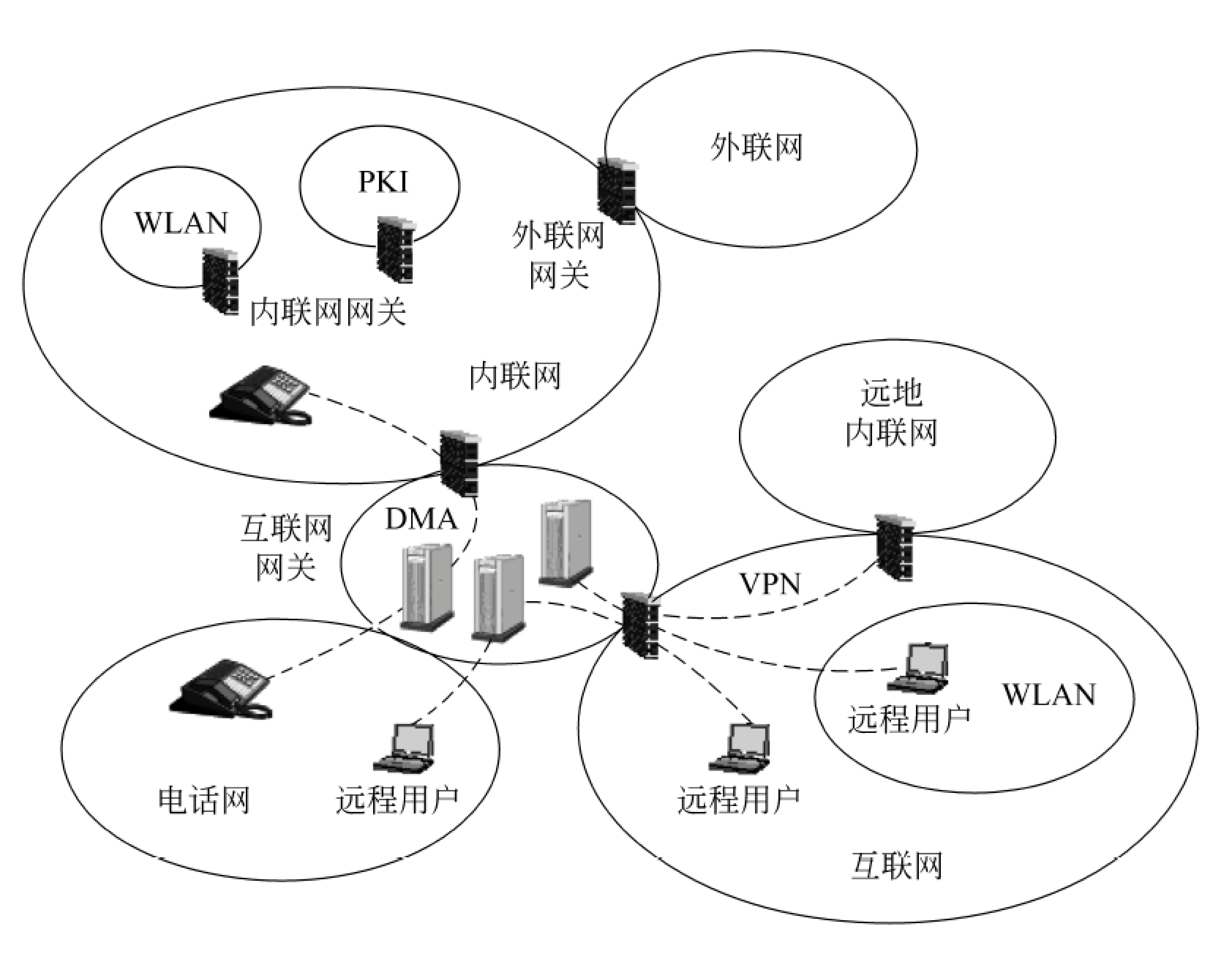


图 19-1　典型的网络环境

高性能价格比的通信和数据交换，提供各种形式的内联网扩展。由于公共网络的信任度低，特别是互联网，因此需要更为复杂的安全网关来管理相关风险。这种安全网关含有特定模块来处理在各种形式的内联网扩展和与合作伙伴及客户连接中的安全要求。

远程用户可采用有线方式或无线方式(例如公共 WLAN)经由互联网接入，也可采用电话拨号经由电话网连接到通常位于互联网防火墙 DMZ 内的远程访问服务器(Remote Access Server)。对于这些接入可采用 VPN(Virtual Private Network)技术实现安全连接。

当一个组织决定使用 VoIP(Voice over IP)技术实现内部电话网时，最好也部署适当的电话网安全网关。

这种典型的网络环境中所采用的技术在许多方面为组织业务提供了扩展的机会和利益，例如减少或优化成本，但同时也使网络环境变得复杂，并常常引入新的信息安全风险。因此，这种风险应得到适当评估，并通过适当的安全控制措施的实施来减轻。也就是说，应平衡新环境带来的机会和新技术引入的风险。

总之，政府机构和商业组织能否成功利用现代网络环境带来的机会，取决于在多大程度上管理和控制这种开放环境中的运行风险。

19.2　网络安全管理过程

在考虑网络连接时，组织内所有对连接负有相关责任的人员都应清楚业务需求和利益。另外，还应意识到这种连接带来的安全风险和相关的控制区域。在考虑网络连接、识别可能的控制区域以及最终选择、设计、实施和维护安全控制措施的过程中所采取的许多

决定和行动都会受到业务需求和利益的影响。因此，在整个过程中应牢记业务需求和利益。为识别适当的网络安全要求和控制区域，应完成如下任务：

- 评审组织的整体信息安全策略中对网络连接的安全要求；
- 评审与网络连接相关的网络体系结构和应用，以为接下来的任务提供必要的背景；
- 识别网络连接的类型；
- 识别网络特性和相关的信任关系；
- 借助于风险评估和管理的评审结果，确定相关安全风险的类型；
- 识别与网络连接类型、网络特性、信任关系和安全风险类型相称的适当的控制区域，同时文件化和评审技术性安全体系结构选项，并确定首选项；
- 实施和运行安全控制措施；
- 持续地监视和评审安全控制措施的实施。

图 19-2 给出了网络安全管理的整个过程。过程中的每一步在接下来的各节中详尽描述。

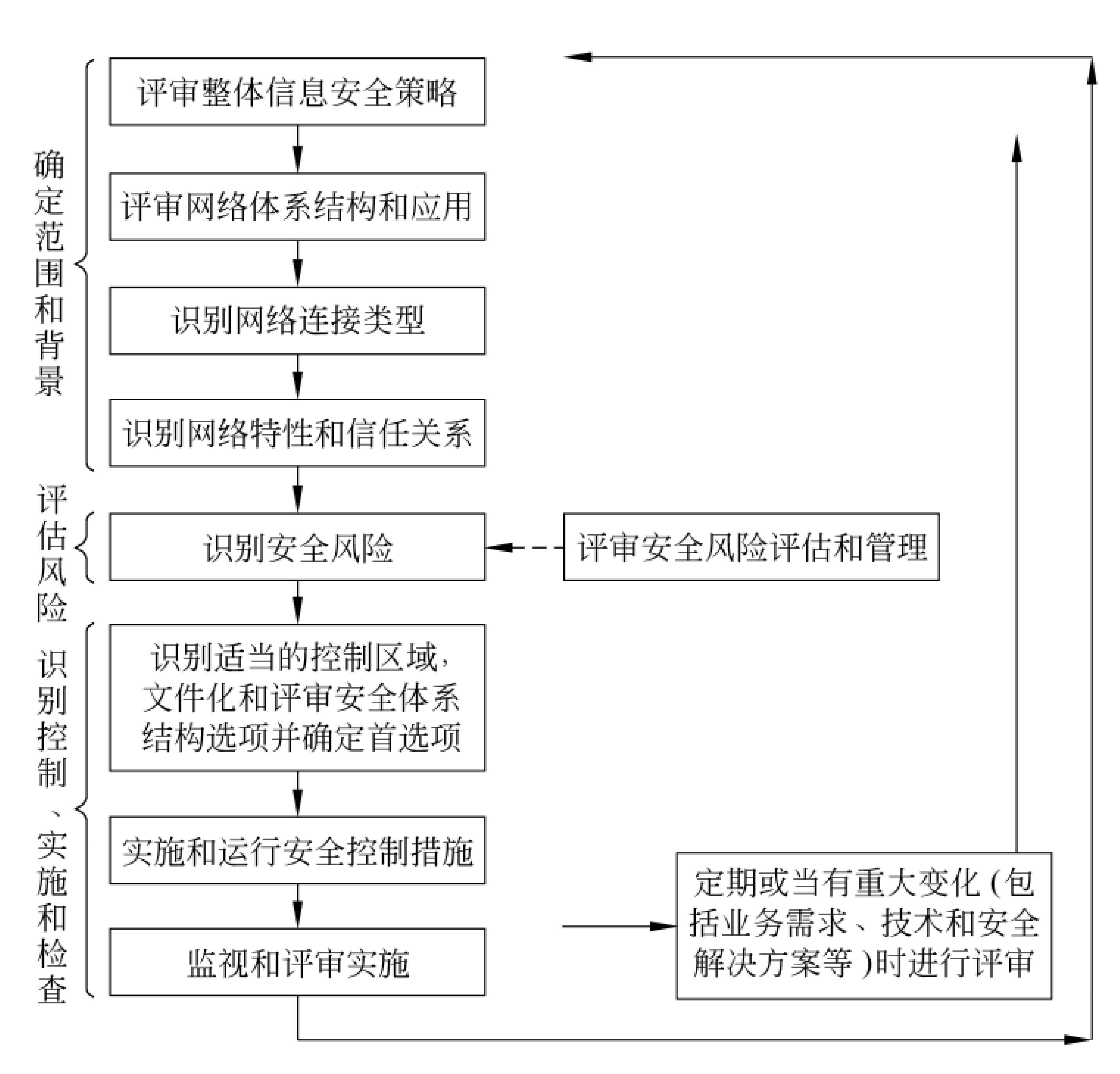


图 19-2　网络安全管理过程

图 19-2 中的实线表示过程的主路径，虚线表示安全风险类型的确定可能借助于安全风险评估和管理的评审结果。

除了过程的主路径外，在某些步骤中需要再审视前面步骤（特别是“评审整体信息安全策略”和“评审网络体系结构和应用”）的结果以确保一致性。例如：

- 在确定安全风险类型之后，可能需要再次评审整体信息安全策略以防出现未被策略层面覆盖的情况。

- 在识别可能的控制区域时，应考虑到整体信息安全策略，因为可能会有因策略需要的特殊控制措施要在组织内全面实施而不考虑风险。
- 在评审安全体系结构选项时，为确保兼容性应考虑网络体系结构和应用。

19.3　评审整体信息安全策略

组织的整体信息安全策略包括与网络连接直接相关的对保密性、完整性、可用性、不可否认性、可核查性、真实性和可靠性需求的陈述，以及对威胁类型的观点和对控制措施的需求。

例如，策略中可能规定：

- 主要关注特定类型的信息和服务的可用性；
- 不允许通过拨号线路进行网络连接；
- 所有到互联网的连接应经过安全网关；
- 应使用某种特殊类型的安全网关；
- 未经过数字签名的支付指令是无效的。

这些适用于整个组织或机构的声明、观点和要求，应在识别网络连接的安全风险（参见第 19.7 节）和控制区域（参见第 19.8 节）过程中被考虑到。如果有任何这种安全要求，应列入可能的控制区域列表中，并在必要时反映在安全体系结构的选项中。

19.4　评审网络体系结构和应用

网络连接类型、网络特性、信任关系、安全风险和控制区域的识别，以及安全体系结构和控制措施的设计，总是在现有或计划的网络体系结构和应用的背景下进行。因此，应获得并评审有关的网络体系结构和应用的详情，以为接下来的这些步骤提供背景和理解。

对网络和应用的体系结构做尽早考虑，可以为评审这些体系结构及当现有体系结构与可接受的安全解决方案发生冲突时可能进行的修改提供充裕的时间。

应考虑的方面包括：

- 网络类型；
- 网络协议；
- 网络应用；
- 网络实现技术；
- 现有网络连接。

1. 网络类型

根据网络覆盖的区域分为：

- 局域网（local area network，LAN），用于连接本地系统；
- 广域网（wide area network，WAN），用于连接直至世界范围的系统。

某些资料将限制在一定区域(如城市)内的 WAN 定义为城域网(metropolitan area network,MAN)。如今两者采用相同的技术,所以 MAN 与 WAN 已没有太大的区别。另外,用于连接个人系统的个人网(personal area network,PAN)在这里被归类为 LAN。

2. 网络协议

不同的网络协议具有不同的安全特性,应加以特别考虑。例如:

- 共享介质协议主要用在 LAN 中为连接的系统使用共享介质提供管理机制。当共享介质被使用时,网络上的所有信息都可被所有连接的系统访问到。
- 路由协议用于定义信息在 WAN 中经过不同节点的传播路径。信息能被沿路的所有系统访问到,并且路由可能会无意或有意地改变。
- MPLS(multi-protocol label switching)协议可使多个专用网络透明地共享一个核心运载网络,即某一专用网络的成员意识不到还有其他专用网络在共享这一核心网络。其主要应用是 VPN,即使用不同的标签来识别被分离的属于不同 VPN 的传输流(注意:基于 MPLS 的 VPN 与基于数据加密机制的 VPN 不同)。

许多网络协议不提供安全性。例如,在公共网络上传输未加密的口令,就很容易被攻击者使用从网络流中获取口令的工具截获。

许多协议被联合使用于不同的网络拓扑和介质,并使用有线和无线技术。在许多情况下,这更进一步地影响到安全特性。

3. 网络应用

网络应用的类型应在安全背景中得到考虑。网络应用类型包括:

- 瘦客户端型的应用;
- 台式机型的应用;
- 基于终端模拟的应用;
- 消息传递型的应用;
- 基于存储转发的应用;
- 客户端/服务器型的应用。

关于应用在其使用的网络环境下,其特性如何影响安全需求,举例如下:

- 消息传递型的应用可能提供了足够的安全性,例如对消息进行加密和数字签名,因而不需要在网络上实施专门的安全控制措施。
- 瘦客户端型的应用可能需要下载移动代码来完成适当的功能。在这种背景下,保密性可能不是主要问题,而完整性是重要的,因此网络可提供适当的机制来保护移动代码的完整。如果有更高的安全要求,另一种选择是对移动代码进行数字签名以提供完整性和真实性。这通常是在应用的自身框架内实现,因而可能无须在网络内提供这种服务。
- 基于存储转发的应用通常将重要数据临时存储在中间节点做进一步处理。如果有完整性和保密性的需求,则在网络中需要有适当的控制措施来保护传输中的数据。然而,由于数据是临时存储在中间节点机上,这些控制措施可能不够。因此,可能还需要另外的控制措施来保护存储在中间节点机上的数据。

4. 网络实现技术

网络可以通过各种技术手段来实现。这些技术手段都是基于网络所覆盖的地理区域来进行构造。网络实现技术包括：

（1）局域网技术

小型 LAN 通常使用共享介质技术。这种情况下，Ethernet 协议是使用的标准技术，并已经被扩展以提供更高的带宽和支持无线环境。对于较大规模的 LAN，鉴于共享介质技术（也包括 Ethernet）的局限性，典型的 WAN 技术（诸如路由协议）也经常被用于 LAN 环境。LAN 可以是基于有线的，也可以是基于无线的。

- 有线 LAN 通常由使用电缆通过网络交换机或集线器连接的节点组成，能提供高速的数据传输能力。众所周知的有线 LAN 技术包括 Ethernet（IEEE 802.3）和令牌环（Token Ring）（IEEE 802.5）。
- 无线 LAN 利用高频无线电波在空中传输网络数据包，其灵活性体现在无须铺设网络线路便可快速建立。众所周知的无线 LAN 技术包括 IEEE 802.11 和蓝牙（bluetooth）。

（2）广域网技术

WAN 可以使用自有电缆和/或服务提供商的线路，或者通过租用远程通信提供商的服务来构成。WAN 技术可以长距离地传输和路由网络流，并提供扩展的路由特性将网络数据包传送到正确的目的 LAN。通常公共的物理联网基础设施用于 LAN 的互联，例如，租用的线路、卫星信道或光纤。WAN 可以是基于有线的，也可以是基于无线的。

- 有线 WAN 通常由经远程通信线路连接到公共或私有网络的路由设备（例如，路由器）组成。众所周知的有线 WAN 技术包括 ATM、帧中继（frame relay）和 X.25。
- 无线 WAN 通常使用无线电波在空中长距离（几十公里或更长）传输网络数据包。众所周知的无线 WAN 技术包括 TDMA、CDMA、GSM 和 IEEE 802.16。

5. 现有网络连接

在评审网络体系结构和应用时，还应考虑组织内外的现有网络连接。组织的现有网络连接可能会因某种原因（例如协议或合同）限制或阻止新的连接。其他网络连接的存在可能会引入额外的脆弱性，并因此面临更高的风险，从而可能需要更强和/或附加的控制措施。

19.5　识别网络连接类型

一个组织或团体可能需要利用的网络连接有多种类型。一些连接可能是通过限于已知团体访问的私有网络建立的，另一些可能是通过可被任何组织或个人访问的公共网络建立。这些网络连接类型可能用于各种服务，例如电子邮件或电子数据交换（electronic data interchange，EDI），可能利用互联网、内联网或外联网设施，每种情况都有不同的安全考虑。每种连接类型会有不同的脆弱性和相关的不同风险，因此最终需要不同的安全

控制措施。

表 19-1 给出了一种从业务角度进行网络连接类型划分的方式。应考虑有关的网络体系结构和应用来选择合适的网络连接类型。由于从业务角度而非技术角度划分网络连接类型，不同的网络连接类型有时可能由类似的技术手段实现，并且在某些情况下所采用的控制措施是类似的，但在其他情况下却不同。

表 19-1　网络连接类型

标识符号	连 接 类 型
A	在一个组织的单一受控场所内的连接
B	在同一组织的不同地理位置之间的连接
C	在一个组织与离开该组织场所进行工作的人员之间的连接
D	在一个封闭团体（如出于合同或法律上的约束或类似的业务兴趣等原因，例如，银行或保险）内不同组织之间的连接
E	与其他组织的连接
F	与一般公共领域的连接
G	从一个 IP 环境到公共电话网的连接

19.6　识别网络特性和信任关系

1. 网络特性

应识别现有或将有网络的特性。识别如下网络特性尤为重要。

- 公共网络：可被任何人访问的网络；
- 私有网络：诸如由自有或租用线路组成的网络，因此被认为比公共网络更安全。

知道网络传输的数据类型也很重要，例如：

- 数据网络：使用数据协议主要传输数据的网络；
- 音频网络：可用于电话但也可传输数据的网络；
- 数据、音频和视频组合网络。

其他相关信息还有：

- 网络是组交换还是线路交换；
- 在 MPLS 网络中是否支持 QoS（Quality of Service）。

2 信任关系

在识别出现有或将有网络的特性（至少识别出网络是公共的还是私有的）之后，就应识别相关的信任关系。

首先，使用如下的简单列表识别与网络连接相关的适用的信任环境：

- 低：诸如与未知用户团体连接的网络；
- 中：诸如与已知用户团体连接或在有多个组织的封闭业务团体内连接的网络；

• 高：诸如只与组织内已知用户团体连接的网络。

其次，将相关的信任环境（低、中和高）关联到适用的网络特性（公共或私有）和网络连接类型（从 A 到 G）来建立信任关系。表 19-2 采用矩阵的形式完成了这种信任关系的建立。

表 19-2　信任关系的识别

网络连接类型		信任环境		
		低	中	高
网络特性	公共	F、G	D、E	B、C
	私有	E	D、E	A、B、C

由表 19-2 可以确定信任关系的参考类别，如表 19-3 所示。

表 19-3　信任关系的参考类别

信任关系类别	描　　述	信任关系类别	描　　述
低/公共	低信任环境并使用公共网络	低/私有	低信任环境并使用私有网络
中/公共	中信任环境并使用公共网络	中/私有	中信任环境并使用私有网络
高/公共	高信任环境并使用公共网络	高/私有	高信任环境并使用私有网络

这些参考类型应被用于确认安全风险和识别控制区域的过程中，必要时辅以网络体系结构和应用方面的可用信息。

19.7　识别安全风险

如前所述，当今大多数组织依靠信息系统和网络的使用来支持其业务运行。在许多情况下，对于网络连接，无论是在组织场所内的信息系统之间，还是到组织内部或外部的其他场所，包括到一般的公共区域，都有明确的业务需求。当组织连接到另一个网络时，应十分注意不要将该组织暴露在另外的风险中，避免潜在威胁利用这一连接所引入的脆弱性。这种风险可能源自网络连接本身，也可能源自网络连接的另一端。

有些风险与确保法律和规章的符合性有关。特别需要关注隐私和数据保护法。

值得关注的安全风险类型包括：

• 未授权访问信息；
• 未授权发送信息；
• 引入恶意代码；
• 否认接受或发起；
• 拒绝服务连接；
• 信息和服务不可用。

当组织面临这些安全风险时可能导致如下安全属性的损失：

- 网络和与网络连接的系统中的信息和代码的保密性；
- 网络和与网络连接的系统中的信息和代码的完整性；
- 信息和网络服务及与网络连接的系统的可用性；
- 网络交易的不可否认性；
- 网络交易的可核查性；
- 信息以及网络用户和管理员的真实性；
- 网络和与网络连接的系统中的信息和代码的可靠性；
- 对未授权使用和挖掘网络资源的可控性。

不是所有安全风险类别都适用于所有场所或所有组织。然而，相关的安全风险类别应予以识别，这样才能识别出可能的控制区域，并最终选择、设计、实施和维护控制措施。

图 19-3 给出了一个表示安全风险类型在哪里发生的网络安全概念模型。

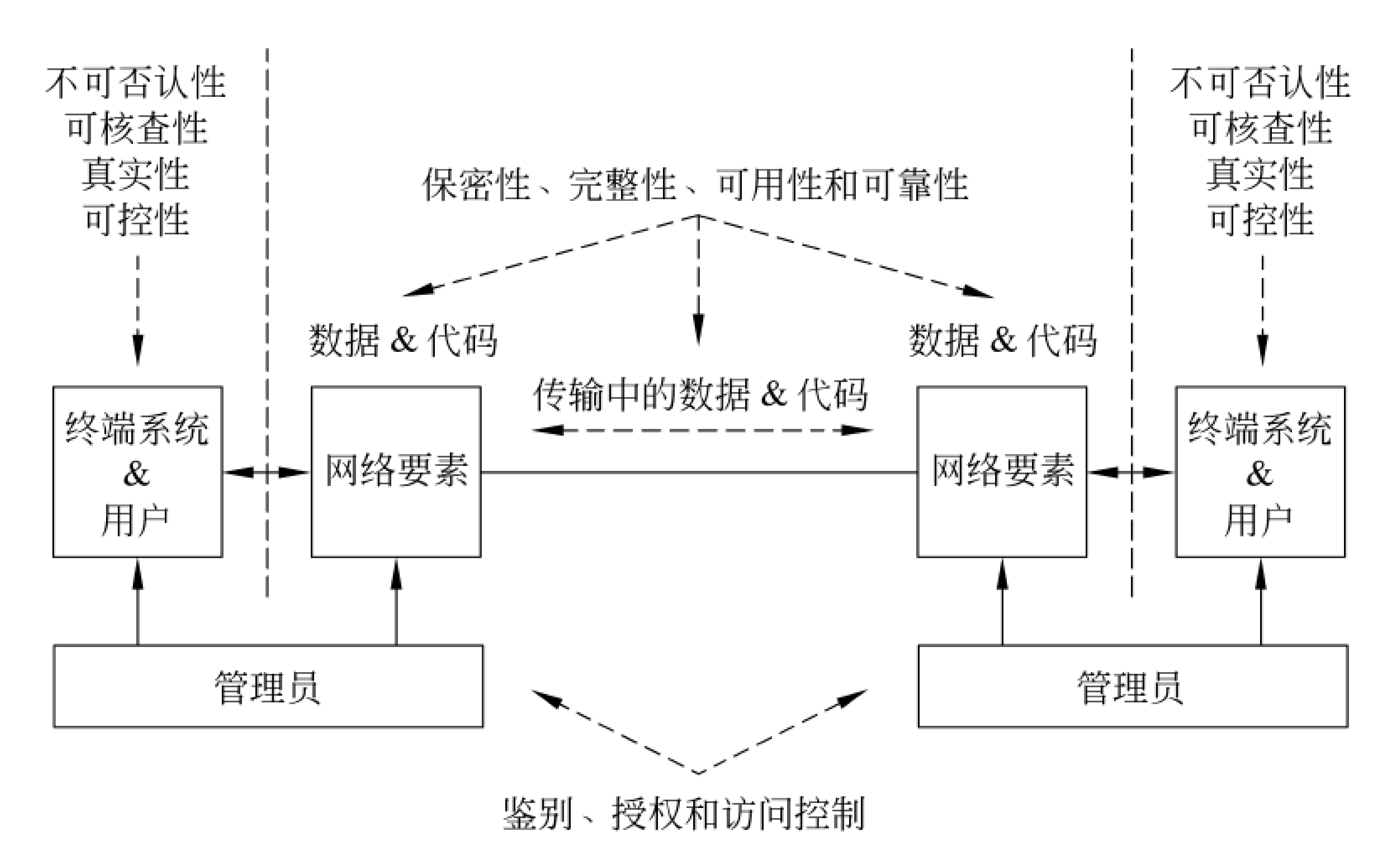


图 19-3　网络安全风险区域的概念模型

应收集与上述安全风险类型有关的业务运行方面的信息，同时考虑业务所涉及信息的敏感性或价值（以对业务的负面影响表示），以及相关的潜在威胁和脆弱性。值得强调的是，在完成识别安全风险这项任务过程中，应利用针对网络连接进行的安全风险评估和管理的评审结果。这些结果有助于在所进行的评审详细程度级别上注视与上述安全风险类型相关的潜在的负面业务影响，所关心的威胁和脆弱性，以及由此得出的风险。

19.8　识别控制区域

基于风险评估和管理的评审结果，加上针对网络所识别的安全风险（参见第 19.7 节），应从本节和 ISO/IEC 27002（即 ISO/IEC 17799）中识别和选择可能的控制区域。实际上，一个特定安全解决方案可能包括多个控制区域。

对于识别出的控制措施，应在相关的网络体系结构和应用的背景下进行充分的评审。在进行了必要的适当调整后，作为实施所需安全控制措施以及监视和评审实施的根据。

本节首先回顾第 5 章已论述的网络安全体系结构，然后介绍各种可能的控制区域。

19.8.1　网络安全体系结构

给出一个安全体系结构参考模型有助于：

- 描述支持网络安全规划、设计和实施的一致框架；
- 定义普遍的安全相关的体系结构要素，并通过适当地应用提供端到端的网络安全。

基于安全体系结构参考模型来描述采用不同现实技术以满足今天和未来需求的实际安全体系结构是有益的。

安全体系结构参考模型中描述的原理适用于任何类型的现代网络，无论是数据、音频还是综合网络，无论是有线还是无线网络，并且能够独立于网络技术或协议来应用。它关注网络基础设施、服务和应用的管理、控制和使用层面上的安全问题，提供一个全面的、自上而下的、端到端的网络安全视角。

安全体系结构参考模型由如下 3 个体系结构组件构成：

- 安全维（又称为安全控制措施组）；
- 安全层（又称为安全要素）；
- 安全面（又称为安全域）。

安全维是一组用来处理网络安全某一特定方面（包括保密性、完整性、可用性、不可否认性、可核查性、真实性、可靠性和可控性）的安全控制措施。

为了提供端到端的安全解决方案，安全维需要应用到网络设备和设施分组的层次结构上，即安全层，包括：

- 基础设施安全层；
- 服务安全层；
- 应用安全层。

安全层以一层建立在另一层上的方式来提供基于网络的安全解决方案，即基础设施安全层支撑服务安全层，服务安全层支撑应用安全层，并通过有层次顺序的网络安全视角来识别应在系统中的哪里实施安全控制。

基础设施安全层由网络传输设施和各网络部件组成，并受到实现安全维的机制保护。基础设施安全层的组件包括路由器、交换机和服务器以及它们之间的通信线路等。

服务安全层关注于服务提供商为其客户提供的服务安全。这些安全服务从基本传输和服务连接（类似于提供互联网访问所必需的服务，例如，鉴别、授权和核查服务，动态主机配置服务，域名服务等）到增值服务（诸如免费电话服务、QoS 和 VPN 等）。

应用安全层聚焦于服务提供商的客户访问网络应用的安全。这些网络应用由网络服务支撑，包括基本的文件传输（如 FTP）和 Web 浏览器应用，目录辅助、基于网络的音频通信和电子邮件这样的基础应用，以及客户关系管理、电子/移动商务、基于网络的培训、视频协作等这样的高端应用。

安全面是指网络活动的类型，并受到实现安全维的机制保护。安全体系结构参考模型定义了如下 3 个安全面来表示受保护网络活动的类型：

- 管理面；
- 控制面；
- 终端用户面。

这些安全面分别关注于与网络管理活动、网络控制活动和终端用户活动相关的特定安全需求。网络设计应尽可能地保持属于不同安全面的活动的适当独立性。

实际的技术性网络安全体系结构与现实网络所采用的各种技术密切相关，包括：

- 局域网(LAN)；
- 广域网(WAN)；
- 无线网 1(Wireless Network)——IEEE 802.11、蓝牙；
- 无线网 2(Radio Network)——TETRA、GSM、3G、GPRS、CDPD 和 CDMA；
- 宽带网(Broadband Network)——3G、电缆、卫星和 DSL；
- 安全网关(Security Gateway)——防火墙；
- VPN(Virtual Private Network)；
- 远程访问服务(Remote Access Service，RAS)——通过互联网通信、拨号 IP 服务；
- IP 综合(数据、音频和视频)——VoIP；
- 外部网络服务访问——电子邮件、互联网服务；
- Web 托管服务(Web Hosting Service)。

通过分析上述技术背景下所面临的安全风险，选择相应的安全控制措施。在最终确定要实施的控制措施之前，应将技术性网络安全体系结构全部形成文件并完全达成一致意见。

19.8.2　网络安全控制区域

1. 安全服务管理框架

任何联网的一个关键安全要求应有发起和控制安全实施和操作的安全服务管理活动的支持。这些活动将确保组织或团体的信息系统所有方面的安全。就网络连接而言，管理活动应包括：

- 定义所有与网络安全相关的责任，指定负有全面责任的一个安全管理者；
- 建立文件化的网络安全策略及其相关的技术性安全体系结构；
- 编制文件化的安全操作规程；
- 进行安全符合性检查，包括安全测试，以确保安全性维持在所要求的水平；
- 为网络连接制定文件化的安全条件，用于在允许与外部组织或人员进行连接时遵守；
- 为网络服务的使用者制定文件化的安全条件；
- 制定文件化并经过测试的业务持续性/灾难恢复计划。

2 网络安全管理

任何网络的管理应在安全的方式下进行，并提供对全面的网络安全管理的支持。为此，需要充分考虑不同的可用网络协议和相关的安全服务。

网络安全管理需考虑如下方面：

- 联网要素，包括网络用户、网络终端系统、网络应用、网络服务和网络基础设施；
- 角色及其责任，包括高级管理、网络管理、网络安全组、网络日常管理员、网络用户和审核员（内部的和/或外部的）；
- 网络监视；
- 网络安全维持，包括及时打安全补丁，定期审核安全控制措施（包括安全测试、漏洞扫描等），以及评价新的网络技术的安全性。

3. 技术脆弱性管理

与其他复杂系统一样，网络系统也会存在错误。网络中常用组件的技术脆弱性如果被利用，会给网络的安全性带来严重影响。技术脆弱性管理应覆盖网络的所有组件，应包括：

- 及时获得有关技术脆弱性的信息；
- 评价网络暴露在这种脆弱性下的程度；
- 确定适当的控制措施来处理相关风险；
- 实施和验证所确定的控制措施。

4. 标识与鉴别

限定仅被授权人员（不管是组织内部的还是外部的）才能经由网络连接进行访问是确保网络服务和相关信息安全的重要手段。与网络连接使用相关的标识与鉴别控制区域包括：

- 远程登录；
- 增强型鉴别；
- 远程系统标识；
- 安全的单点登录。

5. 网络审计日志与监视

通过具有快速检测、调查、报告和相应安全事件的审计日志和持续监视来确保网络安全的有效性是非常重要的。否则，不可能保证网络安全控制措施总是有效的及影响业务运行的安全事件不发生。

对于网络连接，审计日志应包括如下事件类型：

- 失败的远程登录尝试及其日期和时间；
- 失败的再鉴别（或令牌使用）事件；
- 违背安全网关策略的通信；
- 远程尝试访问审计日志；
- 有安全隐患的系统管理报警（例如，IP 地址冲突、线路中断）。

在网络环境下，审计日志的信息有多种来源（如路由器、防火墙和入侵检测系统），并可被送到一个中央审计服务器进行合并和分析。所有的审计日志都应既能实时也能离线查看。

审计踪迹应根据组织的需要在线保留一段时间。所有审计踪迹应以能确保其完整性

和可用性的方式进行备份和存档，如写入 CD 这样的一次写入多次读出（write once read many，WORM）介质。审计日志包含有敏感信息和证据信息，因此有必要予以适当的保护。另外，审计踪迹和相关服务器的时间同步也是重要的。

持续监视应包括如下方面：

- 来自防火墙、路由器、服务器等的审计日志；
- 来自事先设定通知特定事件类型的审计日志的报警；
- 入侵检测系统（intrusion detection system，IDS）的输出；
- 网络安全扫描的结果；
- 用户或维护人员报告的事件信息；
- 安全符合性的评审结果。

网络监视应以完全符合相关国家和国际法律与规章的方式进行。很显然，采取的监视行为应与组织的安全和隐私策略以及具有相关责任的适当规程保持一致。如果网络日志用作刑事或民事起诉的证据，网络审计日志和监视还应按照法律取证的要求进行。

6. 入侵检测

随着网络连接的增加，入侵者有更多入侵途径。此外，入侵者变得更加老练，互联网上有更多容易得到的更加先进的攻击方法和工具。这些工具中的许多是自动的、非常有效的且易于使用的，连经验有限的新手都可以利用。

防止所有的潜在渗透攻击是不可能的，结果是总会发生一些不同程度的成功入侵。对付这种风险除了实施良好的识别与鉴别、逻辑访问控制和核查与审计外，如果合理，还应配以入侵检测能力。这种能力提供预知入侵、识别入侵和发出适当报警的手段。它能够收集入侵信息进行合并和分析，还可以分析出一个组织正常的信息系统行为/使用模式，用以识别异常行为/使用。

在许多情况下，可能清楚某种未授权或有害事件正在发生。它可能是不明原因的服务性能下降，也可能是拒绝特定服务。重要的是要尽可能地知道入侵的原因、严重性和范围，以便采取应对措施。

入侵检测能力相对于审计日志分析工具和方法更加复杂。更加有效的入侵检测能力是使用后台处理器，依据给定的规则，自动分析在审计踪迹和其他日志中记录的过去行为来预知入侵，以及从审计踪迹中分析出恶意行为或非正常使用行为的模式。

入侵检测系统（IDS）有如下两种类型：

- 网络入侵检测系统（network intrusion detection system，NIDS）监视网络上的数据包，并通过与已知攻击模式进行匹配来试图发现入侵行为；
- 主机入侵检测系统（host based intrusion detection system，HIDS）监视主机（服务器）的活动，并通过查看安全事件日志或检查对系统的改变（如对关键系统文件或系统注册表的改变）来发现入侵行为。

在某些情况下，对检测出的入侵的响应可以通过入侵防护系统（intrusion prevention system，IPS）来自动实现。

7. 防范恶意代码

用户应意识到恶意代码（包括病毒）可能通过网络连接进入他们的计算环境。恶意代

码可引起计算机执行非授权的功能(例如,在给定的日期和时间对给定的目标进行消息轰炸)或破坏重要资源(例如删除文件),一旦发现脆弱的主机便在其上复制自己。恶意代码在损害发生之前不太可能被检测出来,除非实施了适当控制。恶意代码可能导致安全控制措施的损害(例如,窃取和泄露口令)、不期望的信息泄露、不期望的信息改变、信息损坏和/或系统资源的非授权使用。

某些恶意代码可以被专门的扫描软件检测出并移除。这种扫描器可用在防火墙、文件服务器、邮件服务器和工作站来封杀某些类型的恶意代码。为了检测出新的恶意代码,通过每天升级确保扫描软件总是最新非常重要。但是,用户和管理员不应指望这种扫描器能够检测出所有恶意代码(甚至某一种类型的所有恶意代码),因为新的恶意代码形式不断出现。通常需要其他形式的控制(如果存在)来加强扫描器所提供的保护。

总体来说,由反恶意代码软件来扫描数据和程序,以识别类似于病毒、蠕虫和木马模式的可疑之处。扫描用的模式库存储着恶意代码的特征,应定期更新或在新的特征可用时进行更新。

带有网络连接的系统的用户和管理员应意识到,当通过外部链路与外部方进行交互时,恶意代码比通常具有更大的风险。应为用户和管理员开发最小化恶意代码引入可能性的规程和实践指南。

用户和管理员应特别小心地配置与网络连接有关的系统和应用,关闭不必要的功能(例如,默认禁止宏操作或在执行宏操作前要求用户确认)。

8. 基于密码基础设施的服务

随着电子副本逐渐代替纸质副本,对电子数据的安全和隐私的保护需求在不断增长。互联网的出现和组织网络扩展到能够让组织外部客户和供应商进行访问,加速了对基于密码的安全解决方案的需求,用来支持鉴别和 VPN 以及确保保密性。

密码基础设施支持的服务包括:

- 网上数据的保密性——采用加密机制实现;
- 网上数据的完整性——采用数字签名和/或数据完整性机制实现;
- 不可否认性——对于一般的不可否认要求,可考虑采用通信协议、应用协议和网关等手段实现,对于较高的不可否认要求,采用数字签名机制实现;
- 密钥管理——采用 PKI,Smartcard 等技术。

9. 业务持续性管理

当灾难发生时,重要的是有控制措施通过提供在适当的时间框架内恢复业务各部分的能力来确保业务持续运行。因此,一个组织应具备业务持续性管理程序,该程序具有覆盖所有的业务持续性阶段的过程,包括建立业务恢复优先级、时间表和要求,明确业务持续性策略,制定业务持续性计划,测试业务持续性计划,确保所有员工的业务持续性意识,维护业务持续性计划和降低风险。

从网络连接视角看,就是要关注维持网络连接,实施具有足够容量的备选连接,在有害事件后恢复连接。这些方面及其要求应基于连接对业务运行的重要程度和中断事件对业务的负面影响。连接性给组织带来许多好处的同时,当发生连接中断事件时,却表现为

脆弱性和单点失效，可能给组织造成破坏性的影响。

19.9　实施和运行安全控制措施

一旦技术性网络安全体系结构及其安全控制措施得到识别、文件化和协商一致，网络安全控制措施就应得到实施。在允许网络运行开始前，实施应得到评审和测试，并且发现的任何安全不足都得到了处理。在安全性得到高层管理批准后，方可投入运行。随着时间的推移及当发生重大变化时，应进行进一步的实施评审。

19.10　监视和评审实施

首次实施应得到评审，以确保与如下文档中规定的技术性安全体系结构和所要求的安全控制措施一致：

- 技术性安全体系结构；
- 联网安全策略；
- 相关的安全运行规程；
- 安全网关服务访问策略；
- 业务连续性计划；
- 安全连接条件。

一致性评审应在投入运行前完成。只有当所有的安全不足被识别、修正并得到高层管理的认可，这种评审才是完整的。投入运行后，也应持续进行监视和评审活动，包括当业务需求、技术和安全解决方案等发生重大变化时和每年定期的活动。

值得强调的是，进行安全测试事先应有安全测试策略和相关的测试计划来确定测试什么、在哪里和什么时间。通常，测试包括漏洞扫描和渗透测试。在开始这种测试前，应检查测试计划，以确保测试将以完全符合相关法律和规定的方式进行。检查时应记住网络可能不局限于一个国家内，它可能分布到具有不同法律的不同国家。测试报告应指出所遇到的脆弱性的详细情况和所需要的修正以及处理的优先级，并附上确认所有修正已经实施的内容。测试报告应得到高层管理的批准。

19.11　本章小结

典型的网络环境包括内联网、外联网、互联网、电话网、无线网和非军事化区（DMZ）。政府机构和商业组织能否成功利用现代网络环境带来机会，取决于在多大程度上管理和控制这种开放环境中的运行风险。

网络安全管理过程包括评审整体信息安全策略、评审网络体系结构和应用、识别网络连接类型、识别网络特性和信任关系、识别安全风险、识别控制区域、实施和运行安全控制

措施、监视和评审实施 8 个步骤。

(1) 评审组织的整体信息安全策略中对网络连接的安全要求。组织的整体信息安全策略包括与网络连接直接相关的对保密性、完整性、可用性、不可否认性、可核查性、真实性和可靠性需求的陈述，以及对威胁类型的观点和对控制措施的需求。

(2) 评审网络体系结构和应用时应考虑网络类型、网络协议、网络应用、网络实现技术和现有网络连接等方面。网络类型包括局域网和广域网；网络协议包括共享介质协议、路由协议和 MPLS；网络应用包括瘦客户端型、台式机型的应用、基于终端模拟的应用、消息传递型的应用、基于存储转发的应用和客户端/服务器型的应用；网络实现技术包括有线/无线局域网/广域网技术；现有网络连接可能影响新的连接。

(3) 考虑到有关的网络体系结构和应用，选择合适的网络连接类型。网络连接类型从业务角度按照连接的对象和范围被划分为 A～G 这 7 种类型。

(4) 根据网络连接类型(从 A 到 G)确定信任环境(低、中和高)，再关联到网络特性(公共或私有)建立信任关系，包括低/公共、中/公共、高/公共、低/私有、中/私有和高/私有六个参考类别。

(5) 借助于风险评估和管理的评审结果，确定相关安全风险的类型，包括未授权访问信息、未授权发送信息、引入恶意代码、否认接受或发起、拒绝服务连接、信息和服务不可用等。

(6) 根据网络连接类型、网络特性、信任关系和安全风险类型，识别相应的控制区域和控制措施，并在相关的网络体系结构和应用的背景下进行充分的评审和必要的适当调整。

(7) 实施选定的安全控制措施，并在网络投入运行前，对实施结果进行评审和测试，解决发现的任何安全不足。在安全性得到高层管理批准后，方可投入运行。

(8) 持续监视，并定期和当发生重大变化时评审网络安全，以判断是否仍然满足要求。

习　　题

1. 简述网络安全管理过程。
2. 网络连接类型是如何划分的?
3. 如何识别网络环境中的信任关系? 信任关系有哪些类型?
4. 阐述安全风险识别的用途和作用。
5. 列出网络安全的控制区域。
6. 何时进行评审活动?
7. 对于安全测试有哪些注意事项?

第20章 安全认证和评估

本章要点：

- 风险管理和过程；
- 安全成熟度模型的作用和构成；
- 威胁来源、威胁方法及预防对策；
- 安全评估过程的主要阶段；
- 网络安全评估技术；
- 安全评估准则概况。

针对内部和外部的攻击所采用的安全体系结构的能力需要认证和评估。技术在不断变化，新的应用正在开发，新的平台正在加到非军事区(DMZ)，额外的端口正在加进防火墙。由于竞争，很多应用在市场的生存时间越来越短，软件开发生命周期中的测试和质量保证正在忽略。很多大的组织甚至没有一个完全的目录，将计算机、网络设备以及在网络上的各个应用编制进去，而只是将这些组件独自地进行配置。由于没有将安全测试作为软件质量保证的一个组成部分，应用的漏洞(脆弱性)不断发生。

安全评估认证安全体系结构是否能满足安全策略和最好的经营业务实际。一个典型的安全评估问题是它经常没有用于对经营业务的影响的评析。这里引入一个概念，称为安全成熟度模型(Security Maturity Model，SMM)，用来适当地测量一个给定的准则，该准则基于在工业界最佳的经营业务实际，且能将其反馈到经营业务。它还提供一个改进的方法，包括将不足之处列成清单。安全成熟度模型可测量企业安全体系结构的3个不同部分：安全计划、技术和配置、操作运行过程。

从经营业务的观点看，要求安全解决方案的性能价格比最好，即基于特定产业的最佳实际。在任何系统中的安全控制应预防经营业务的风险。然而，决定哪些安全控制是合适的以及性能价格比好的这一过程经常是复杂的，有时甚至是主观的。安全风险分析的最主要功能是将这个过程置于更为客观的基础上。

20.1 风险管理

风险管理是识别、评估和减少风险的过程。一个组织有很多个体负责对给定应用接受给定风险。这些个体包括总经理、CFO(Chief Financial Officer，首席财务执行官)、经营业务部门的负责人，以及信息所有者。一个组织的总的风险依赖于下面一

些属性：

- 资产的质量（丢失资产的效应）和数量（钱）的价值；
- 基于攻击的威胁可能性；
- 假如威胁实现，对经营业务的影响。

将资产价值和代价相联系或决定投资回报（Return On Investment，ROI）的能力经常是困难的。相反，可以确定保护机制的代价。将国家秘密的信息作为极敏感的信息，因为对这些信息的错误处理，其结果将危害到国家秘密。比之于商业组织，政府愿意花更多的费用来保护信息。

直接的定量花费包括更换损坏的设备、恢复后备和硬盘的费用等。由于事故而引起的宕机时间是可测量的，很多金融贸易系统因此而遭受大量经济损失。生产的降低，例如 E-mail 服务器宕机，很多组织的工作将停止。

与定量的代价相比，质量的代价对组织的破坏更大。假如用来销售的 Web 站点被黑客破坏了，有可能所有客户的信用卡号被偷，这将严重地影响这个站点的信誉。也有可能在短时期内，经营业务停止。

风险评估对漏洞和威胁的可能性进行检查，并考虑事故造成的可能影响。威胁的水平决定于攻击者的动机、知识和能力。大部分内部人员不大可能使用黑客工具，然而十分熟悉网上的应用，可以删除文件、引起某些物理损坏，甚至是逻辑炸弹等。

漏洞水平和保护组织资产的安全体系结构的能力正相反。如果安全控制弱，那么暴露的水平高，随之发生事故灾难的几率也大。对数据、资源的漏洞及其利用的可能性取决于以下属性，且很难预测：资产的价值、对对手的吸引力、技术的变更、网络和处理器的速度、软件的缺陷等。

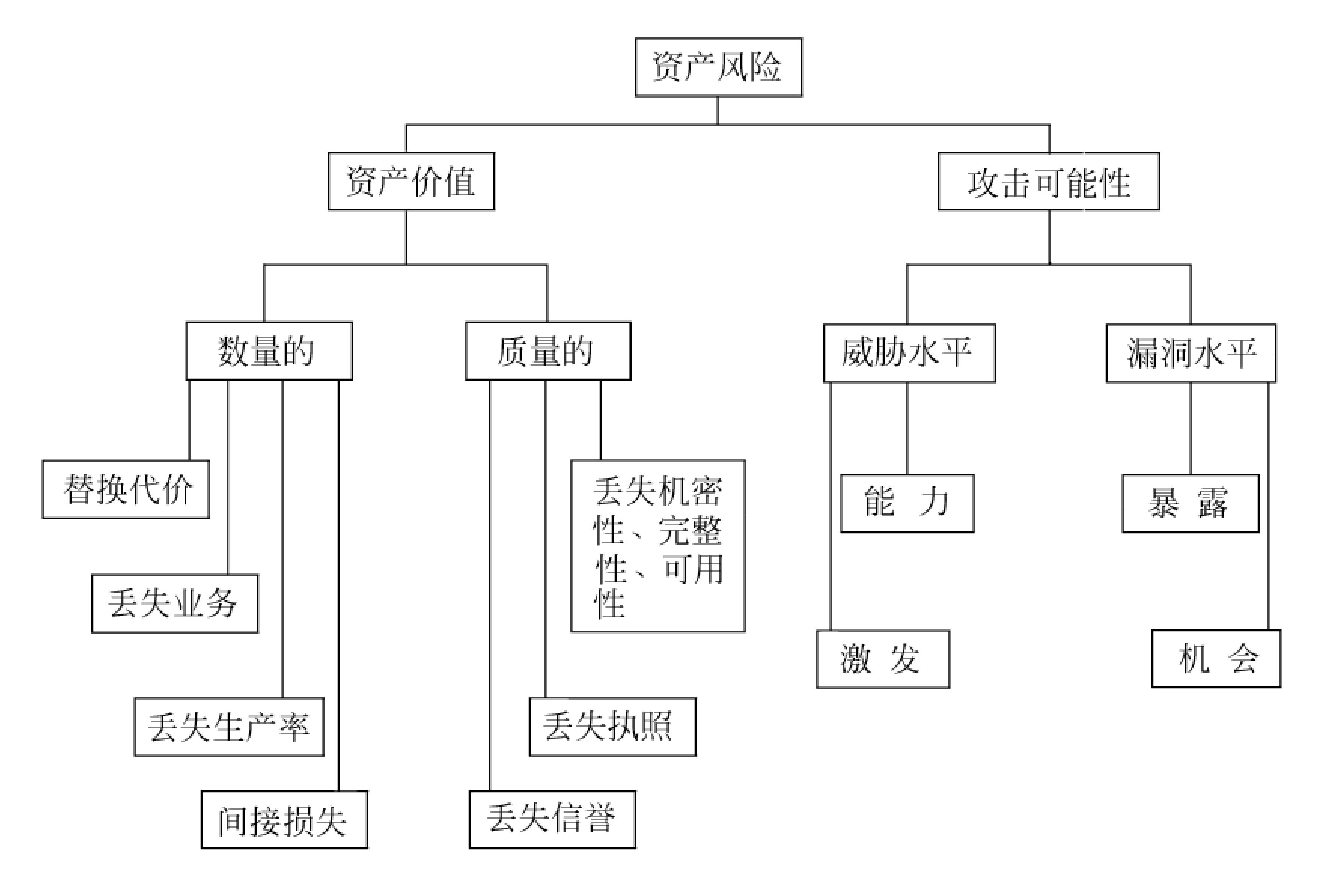


图 20-1　风险评估方法

描述威胁和漏洞最好的方法是根据对经营业务的影响描述。此外,对特殊风险的评估影响还和不确定性相联系,也依赖于暴露的水平。所有这些因素对正确地预测具有很大的不确定性,因此安全的计划和认证是十分困难的。图 20-1 表示了风险评估的方法。

20.2 安全成熟度模型

成熟度模型可用来测量组织的解决方案(软件、硬件和系统)的能力和效力。因此它可用于安全评估,以测量针对业界最佳实际的安全体系结构。可以就以下 3 个方面进行分析:安全计划、技术和配置、操作运行过程。安全计划包括安全策略、标准、指南以及安全需求。技术和配置的成熟度水平根据选择的特定产品、准则,在组织内的安置以及产品配置而定。操作运行过程包括变更管理、报警和监控,以及安全教育方面。美国 Carnegie Mellon 大学的软件工程研究所(Software Engineering Insititue,SEI)制定了系统安全工程能力成熟度模型(System Security Engineering Capability Maturity Model, SSE-CMM)。它将安全成熟度能力级别分成 4 级,以适应不同级别的安全体系结构,如表 20-1 所示。

1. 安全计划

一个好的安全体系结构必须建立在一个坚固的安全计划基础之上。计划的文本必须清晰、完整。很多组织的安全策略、标准和指南存在以下一些问题:

(1) 内容太旧,已过时,不适用于当前的应用。安全策略应每年更新,以适应技术的变化。

表 20-1　安全成熟度能力级别

安全成熟度能力级别	说　　明
无效力(50%)	总的安全体系结构没有遵从企业安全策略、法规,以及最佳经营实际
需要改进(65%)	安全体系结构中无效力的应少于 35%
合适(85%)	企业的安全计划、部署、配置和过程控制使安全体系结构能满足总的目标
极好(超过 100%)	安全体系结构超过了总的目标及需求

(2) 文本有很多用户,如开发者、风险管理者、审计人员,所用语言又适用于多种解释。如果陈述太抽象,那么实施时将无效力。

(3) 表达不够详细。很多组织的安全策略观念只是一个口令管理。组织安全策略文本中通常缺少信息的等级分类以及访问控制计划文本。

(4) 用户需要知道有关安全的文本。如果用户不能方便地获得和阅读文本,就会无意地犯规,然而难以追查责任。

2 技术和配置

当今,市场上有很多安全厂商和安全产品,但是没有一个产品能提供完全的安全解决方案。诸如防火墙、IDS、VPN、鉴别服务器等产品都只是解决有限的问题。安全专业人员应能适当地选择产品,正确地将它们安置在基础设施中,合适地配置和支持。然而,他们经常会不正确地采购安全产品,例如,有人认为只要在需要保护的有价值的资产前放置一个防火墙,就什么问题都能解决。从网络的观点看部分正确,但防火墙不提供应用和平台的保护,也不提供有用的入侵检测信息。

安全产品的合适配置也是一个挑战。有时产品的默认配置是拒绝所有访问,只有清晰的允许规则能通过通信。安全产品配置的最大挑战是需要有熟练的专业人员来配置和管理。

3 运行过程

运行过程包括安全组件需要的必要支持和维护、变更管理、经营业务的连续性、用户安全意识培训、安全管理,以及安全报警与监控。安全基础设施组件的支持和维护类似于主机和应用服务器所需的支持。允许的变更管理要有能退回到目前工作版本的设施,并且要和经营业务连续性计划协调一致。

安全设备会产生一些不规则的日志信息,这对管理员来说是复杂的,一旦配置有差错,就会阻止访问网络、应用或平台。对各种人员的培训是任何安全体系结构成功的关键。最后,识别安全事故的能力且按照一个逐步升级的过程来恢复是最重要的。

技术变化十分迅速,对从事于安全事业的人员增加了很多困难,因此选择高水平的人员从事该项工作是必需的。特别是,从事安全培训的专业人员是有效信息安全程序的关键,要使用各种有效媒体进行安全培训课程。每个企业员工都要接受安全培训,要对不同的人员(例如安全管理员、最终用户、数据拥有者)有针对性地进行培训。

20.3　威胁

在第 2 章中讲到,风险是构成安全基础的基本观念。风险是丢失需要保护的资产的可能性。测定风险的两个组成部分是漏洞和威胁。漏洞是攻击可能的途径,威胁是一个可能破坏信息系统安全环境的动作或事件。威胁包含 3 个组成部分:

(1) 目标,可能受到攻击的方面。

(2) 代理,发出威胁的人或组织。

(3) 事件,做出威胁的动作类型。作为威胁的代理,必须要有访问目标的能力,有关于目标的信息类型和级别的知识,还要有对目标发出威胁的理由。

本章从安全的验证和评估出发,具体分析各种威胁源、威胁是如何得逞的以及针对这些威胁的对策。

20.3.1　威胁源

弄清楚威胁的来源是减少威胁得逞可能性的关键,下面陈述各种主要的威胁源。

1. 人为差错和设计缺陷

最大的威胁来源是操作中人为的疏忽行为。据一些统计，造成信息系统在经费和生产力方面损失的一半是由于人为的差错，另一半则是有意的、恶意的行为。这些人为差错包括不适当地安装和管理设备、软件，不小心地删除文件，升级错误的文件，将不正确的信息放入文件，忽视口令更换或做硬盘后备等行为，从而引起信息的丢失、系统的中断等事故。

上述事故由于设计的缺陷，没有能防止很多普遍的人为差错引起的信息丢失或系统故障。设计的缺陷还会引起各种漏洞的暴露。

2. 内部人员

很多信息保护设施的侵犯是由一些试图进行非授权行动或越权行动的可信人员执行的。其动机有些是出于好奇，有些是恶意的，有些则是为了获利。内部人员的入侵行为包括复制、窃取或破坏信息，然而这些行为又难以检测。这些个体持有许可或其他的授权，或者通过那些无须专门授权的行为使网络运行失效或侵犯保护设施。根据统计，内部人员的侵犯占所有严重安全侵犯事件的 70%～80%。

3. 临时员工

外部的顾问、合同工、临时工应和正式员工一样，必须有同样的基本信息安全要求和信息安全责任，但还需有一些附加的限制。例如，和正式员工一样，需签一个信息安全遵守合同，接受相应的安全意识培训。除此之外，临时员工还必须有一个专门的协议，只允许访问那些执行其委派的任务所需的信息和系统。

4. 自然灾害和环境危害

环境的要求，诸如最高温度和最低温度、最高湿度、风暴、龙卷风、照明、为水所淹、雨、火灾以及地震等，都能破坏主要的信息设施及其后备系统。应制定灾难恢复计划，预防和处理这些灾害。

5. 黑客和其他入侵者

来自于非授权的黑客，为了获得钱财、产业秘密或纯粹是破坏系统的入侵攻击行为近年来呈上升趋势。这些群体经常雇佣一些攻击高手并进行耸人听闻的报道。这些群体包括青少年黑客、专业犯罪者、工业间谍或外国智能代理等。

6. 病毒和其他恶意软件

病毒、蠕虫、特洛伊木马以及其他恶意软件通过磁盘、预包装的软件、电子邮件和连接到其他网络进入网络。这些危害也可能是由于人为差错、内部人员或入侵者引起的。

20.3.2 威胁情况与对策

采取对策以防止各种威胁情况，不仅需要了解威胁的来源，还应知道这些威胁是怎样侵袭安全体系结构的。下面列举各种情况。

1. 社会工程（系统管理过程）

社会工程攻击假冒已知授权的员工，采用伪装的方法或电子通信的方法，具体情况

如下：

① 攻击者发出一封电子邮件，声称是系统的根，通知用户改变口令以达到暴露用户口令的目的。

② 攻击者打电话给系统管理员，声称自己是企业经理，丢失了 modem 池的号码、忘记了口令。

③ 谎说是计算机维修人员，被批准进入机房，并访问系统控制台。

④ 含有机密信息的固定存储介质（硬盘、软盘）被丢弃或不合适地标号，被非授权者假装搜集废物获得。

所有上面 4 种威胁情况都可以使攻击得逞。社会工程的保护措施大多是非技术的方法。下面列出的每一种保护措施可防御上面提到的攻击：

（1）培训所有企业用户的安全意识。

（2）培训所有系统管理员的安全意识，并有完善的过程、处理、报告文本。

（3）对允许外访人员进入严格限制区域的负责人进行安全意识培训。

2. 电子窃听

Internet 协议集在设计时并未考虑安全。TELNET、FTP、SMTP 和其他基于 TCP/IP的应用易于从被动的线接头获取。用户鉴别信息（如用户名和口令）易于从网络中探测到，并伪装成授权员工使用。假如外部人员对企业设施获得物理访问，则可以将带有无线 modem 的手提计算机接到局域网或集线器上，所有通过局域网或集线器的数据易于被任何威胁者取得。此外，假如外部人员能电子访问带有 modem 服务器进程的工作站，就可以将其作为进入企业网络的入口。任何在 Internet 传输的数据对泄露威胁都是漏洞。所有上述 4 种威胁都有可能使这些攻击得逞。

防止窃听的保护措施包括鉴别和加密。使用双因子鉴别提供强的鉴别，典型的做法是授权用户持有一个编码信息的物理标记再加上一个用户个人标识号（PIN）或口令。保护传输中的口令和 ID，可以采用加密的措施。链路加密（SSL 和 IPv6）保护直接物理连接或逻辑通信通路连接的两个系统之间传输的信息。应用加密（安全 Telnet 和 FTP、S/MIME）提供报文保护，在源端加密，只在目的地解密。数字签名可认证发送者的鉴别信息，如伴随用哈希算法可保护报文的完整性。

3. 软件缺陷

当前两个最大的软件缺陷是缓冲器溢出和拒绝服务攻击。当写入太多的数据时，就会发生缓冲器溢出，通常是一串字符写入固定长度的缓冲器。对数据缓冲器的输入没有足够的边界检查，使得输入超过缓冲器的容量。一般情况下，系统崩溃是由于程序试图访问一个非法地址。然而，也有可能用一个数据串来代替生成可检测的差错，从而造成攻击者希望的特定系统的漏洞。Carnegie Mellon 软件工程研究所的计算机应急响应组（Computer Emergenoy Response Team，CERT）有 196 个有关缓冲器溢出的文档报告，如 Microsoft 的终端服务器 Outlook Express，Internet 信息服务器（IIS），还有一些众人熟知的有关网络服务的，如网络定时协议（Network Time Protocol，NTP）、Sendmail、BIND、SSHv1.37、Kerberos 等。

一个拒绝服务攻击使得目标系统响应变慢，以致完全不可用。有很多原因可导致这种结果：①编程错误以致使用 100％的 CPU 时间。②由于内存的漏洞使系统的内存使用连续增加。③Web 请求或远程过程调用(RPC)中发生的畸形数据请求。④大的分组请求，如大量电子邮件地址请求和 Internet 控制报文协议(Internet Control Message Protocol，ICMP)请求。⑤不停的网络通信 UDP 和 ICMP 造成广播风暴和网络淹没。⑥伪造的路由信息或无响应的连接请求。⑦布线、电源、路由器、平台或应用的错误配置。

CERT 有 318 个文本是关于对各种应用和平台操作系统的拒绝服务攻击。在大多数情况下，由于攻击者已经损坏了执行攻击的机器，使得要告发这些个体实施的攻击很困难。

4. 信任转移(主机之间的信任关系)

信任转移是把信任关系委托给可信的中介。一旦外部人员破坏了中介信任的机器，其他的主机或服务器也易于破坏。这样的攻击例子如下：①误用一个. rhosts 文件使受损的机器不需口令就能攻击任何在 . rhosts 文件中的机器。②假如外面的用户伪装成一个网络操作系统用户或服务器，则所有信任该特定用户或服务器的其他服务器也易于受破坏。③一个通过网络文件系统(Network File System，NFS)由各工作站共享文件的网络，假如其中一个客户工作站受损，一个攻击者能在文件系统服务器上生成可执行的特权，那么攻击者能如同正常用户一样登录服务器并执行特权命令。

信任转移的保护措施主要是非技术方法。大部分 UNIX 环境(非 DCE)不提供信任转移的自动机制。因此系统管理员在映射主机之间的信任关系时必须特别小心。

5. 数据驱动攻击(恶意软件)

数据驱动攻击是由嵌在数据文件格式中的恶意软件引起的。这些数据文件格式如 PS 编程语言(postscript)文件、在文本中的 MS Word 基本命令、shell 命令表(shell script)，下载的病毒或恶意程序。数据驱动攻击的例子如下：

① 一个攻击者发送一个带有文件操作的 postscript 文件，将攻击者的主机标识加到. rhosts文件；或者打开一个带有 Word 基本命令的 MS Word 文本，能够访问 Windows 动态链接库(Dynamic Link Library，DLL)内的任何功能，包括 Winsock. dll。

② 一个攻击者发送一个 postscript 文件，该文件常驻在基于 postscript 的传真服务器中，就能将每一个发送和接收的传真拷贝发送给攻击者。

③ 一个用户从网上下载 shellscript 或恶意软件，将受害者的口令文件邮寄给攻击者，并删除所有受害者的文件。

④ 利用 HTTP 浏览器包装诸如特洛伊木马等恶意软件。

6. 拒绝服务

DoS 攻击并不利用软件的缺陷，而是利用实施特定协议的缺陷。这些攻击会中断计算平台和网络设备的运行，使特定的网络端口、应用程序(如 SMTP 代理)和操作系统内核超载。这些攻击的例子有 TCP SYN 淹没、ICMP 炸弹、电子邮件垃圾、Web 欺骗、域名

服务(Domain Name System,DNS)拦劫等。保持计算平台和网络设备的及时更新能避免大多数这些攻击。防止有一些攻击需要诸如网络防火墙这类网络过滤系统。

7. DNS 欺骗

域名系统(DNS)是一个分布式数据库,用于 TCP/IP 应用中,映射主机名和 IP 地址,以及提供电子邮件路由信息。如果 Internet 地址值到域名的映射绑定过程被破坏,域名就不再是可信的。这些易破坏的点是讹用的发送者、讹用的接收者、讹用的中介,以及服务提供者的攻击。例如,假如一个攻击者拥有自己的 DNS 服务器,或者破坏一个 DNS 服务器,并加一个含有受害者.rhosts 文件的主机关系,攻击者就很容易登录和访问受害者的主机。

对 DNS 攻击的保护措施包括网络防火墙和过程方法。网络防火墙安全机制依靠双 DNS 服务器,一个用于企业网络的内部,另一个用于外部,即对外公开的部分。这是为了限制攻击者了解内部网络主机的 IP 地址,从而加固内部 DNS 服务。Internet 工程任务组(Internet Engineering Task Force,IETF)正致力于标准安全机制工作以保护 DNS。所谓反对这些攻击的过程方法是对关键的安全决定不依赖于 DNS。

8. 源路由

通常 IP 路由是动态的,每个路由器决定将数据报发往下面哪一个站。但 IP 的路由也可事先由发送者来确定,称源路由。严格的源路由依赖于发送者提供确切的通路,IP 数据报必须按此通路走。松散的源路由依赖于发送者提供一张最小的 IP 地址表,数据报必须按该表的规定通过。攻击者首先使受害者可信主机不工作,假装该主机的 IP 地址,然后使用源路由控制路由到攻击者主机。受害者的目标主机认为分组来自受害者的可信主机。源路由攻击的保护措施包括网络防火墙和路由屏幕。路由器和防火墙能拦阻路由分组进入企业网络。

9. 内部威胁

内部威胁包括前面提到的由内部人员作恶或犯罪的威胁。大多数计算机安全统计表明,70%～80%的计算机欺骗来自内部。这些内部人员通常有反对公司的动机,能对计算机和网络进行直接物理访问,以及熟悉资源访问控制。在应用层的主要威胁是被授权的人员滥用和误用授权。网络层的威胁是由于能对 LAN 进行物理访问,使内部人员能见到通过网络的敏感数据。

针对内部威胁的防护应运用一些基本的安全概念:责任分开、最小特权、对个体的可审性。责任分开是将关键功能分成若干步,由不同的个体承担,如财务处理的批准、审计、分接头布线的批准等。最小特权原则是限制用户访问的资源,只限于工作必需的资源。这些资源的访问模式可以包括文件访问(读、写、执行、删除)或处理能力(系统上生成或删除处理进程的能力)。个体的可审性是保持各个体对其行为负责。可审性通常是由系统的用户标识和鉴别以及跟踪用户在系统中的行为来完成。

20.4 安全评估方法

20.4.1 安全评估过程

当前安全体系结构的能力水平应从安全成熟度模型的 3 个方面进行评估，即对计划、布局和配置、运行过程的评估。安全评估方法的第 1 步是发现阶段，所有有关安全体系结构适用的文本都必须检查，包括安全策略、标准、指南，信息等级分类和访问控制计划，以及应用安全需求。全部基础设施安全设计也须检查，包括网络划分设计，防火墙规则集，入侵检测配置；平台加固标准、网络和应用服务器配置。

评估的第 2 步是人工检查阶段，将文本描述的体系结构与实际的结构进行比较，找出其差别。可以采用手工的方法，也可采用自动的方法。使用网络和平台发现工具，在网络内部执行，可表示出所有的网络通路以及主机操作系统类型和版本号。NetSleuth 工具是一个 IP 可达性分析器，能提供到网络端口级的情况。QUESO 和 NMAP 这些工具具有对主机全部端口扫描的能力，并能识别设备的类型和软件版本。

评估的第 3 步是漏洞测试阶段。这是一个系统的检查，以决定安全方法的适用、标识安全的差别、评价现有的和计划的保护措施的有效性。漏洞测试阶段又可分成 3 步。第 1 步包括网络、平台和应用漏洞测试。网络漏洞测试的目标是从攻击者的角度检查系统。可以从一个组织的 Intranet 内，也可以从 Internet 的外部，或者一个 Extranet 合作伙伴进入组织。用于网络漏洞测试的工具通常是多种商业化的工具（例如 ISS 扫描器、Cisco 的 Netsonar）以及开放给公共使用的工具（例如 Nessus 和 NMAP）。这些测试工具都以相同的方式工作。首先对给出的网络组件（例如防火墙、路由器、VPN 网关、平台）的所有网络端口进行扫描。一旦检测到一个开启的端口，就使用已知的各种方法攻击这端口（例如在 Microsoft IIS 5.0、Kerberos、SSHdaemon 和 Sun Solstice AdminSuite Daemon 的缓冲器溢出）。大部分商业产品能生成一个详细的报告，根据攻击产生的危害，按风险级别列出分类的漏洞。漏洞测试的第 2 步是平台扫描，又称系统扫描。平台扫描验证系统配置是否遵守给定的安全策略。此外，它还检测任何安全漏洞和配置错误（例如不安全的文件保护——注册和配置目录）以及可利用的网络服务（例如 HTTP、FTP、DNS、SMTP 等）。一旦平台的安全加固已经构建，系统扫描将构成基础，它定时地检测任何重要的变化（例如主页更换、Web 站点受损）。漏洞测试的第 3 步是应用扫描。应用扫描工具不像网络或平台工具那样是自动的，因此，它是一个手动的处理过程。其理念是模仿攻击者成为授权用户是如何误用这应用。

安全评估的最后 1 步是认证安全体系结构的处理过程部分。包括自动的报警设施以及负责配置所有安全体系结构组件（如防火墙、IDS、VPN 等）的人。安全控制出现问题最多的是人为的差错。例如，引起防火墙不能安全运行的主要原因是配置的错误以及不好的变更管理过程，如下面一些情况：①有一个防火墙管理员在深夜接到一个紧急电话，声称由于网络的问题使应用出错。②管理员取消管理集对分组的限制，观察是否是防火墙阻断了这个分组。③应用开始正常工作，管理员回去睡觉，但忘了防火墙管理集是打开着的。④之后企业网络被入侵，因为防火墙并不执行任何访问控制。

在漏洞分析测试期间，安全体系结构监控和报警设施应在最忙的状态。测试可以事先通知，允许净化安全日志、分配合适的磁盘空间。测试也可以事先不通知，可以测量安全支持人员的反应时间。测量 Internet 服务提供者的反应时间是有用的，特别是他们负责管理 Internet 防火墙的情况。

将上面 5 个漏洞分析测试阶段的结果汇总、分析，可得出总的风险分析文本，从 5 个阶段中产生的信息是覆盖的。很多自动工具厂商有内置的报告产生器，根据可能引起危害的漏洞进行分类。风险分析信息必须应用到经营业务，转而成为经营业务影响的文本。很多安全评估报告没有将风险分析反馈到对经营业务的影响，安全评估的价值就很小。图 20-2 表示从安全成熟度模型 3 个方面的安全评估阶段。

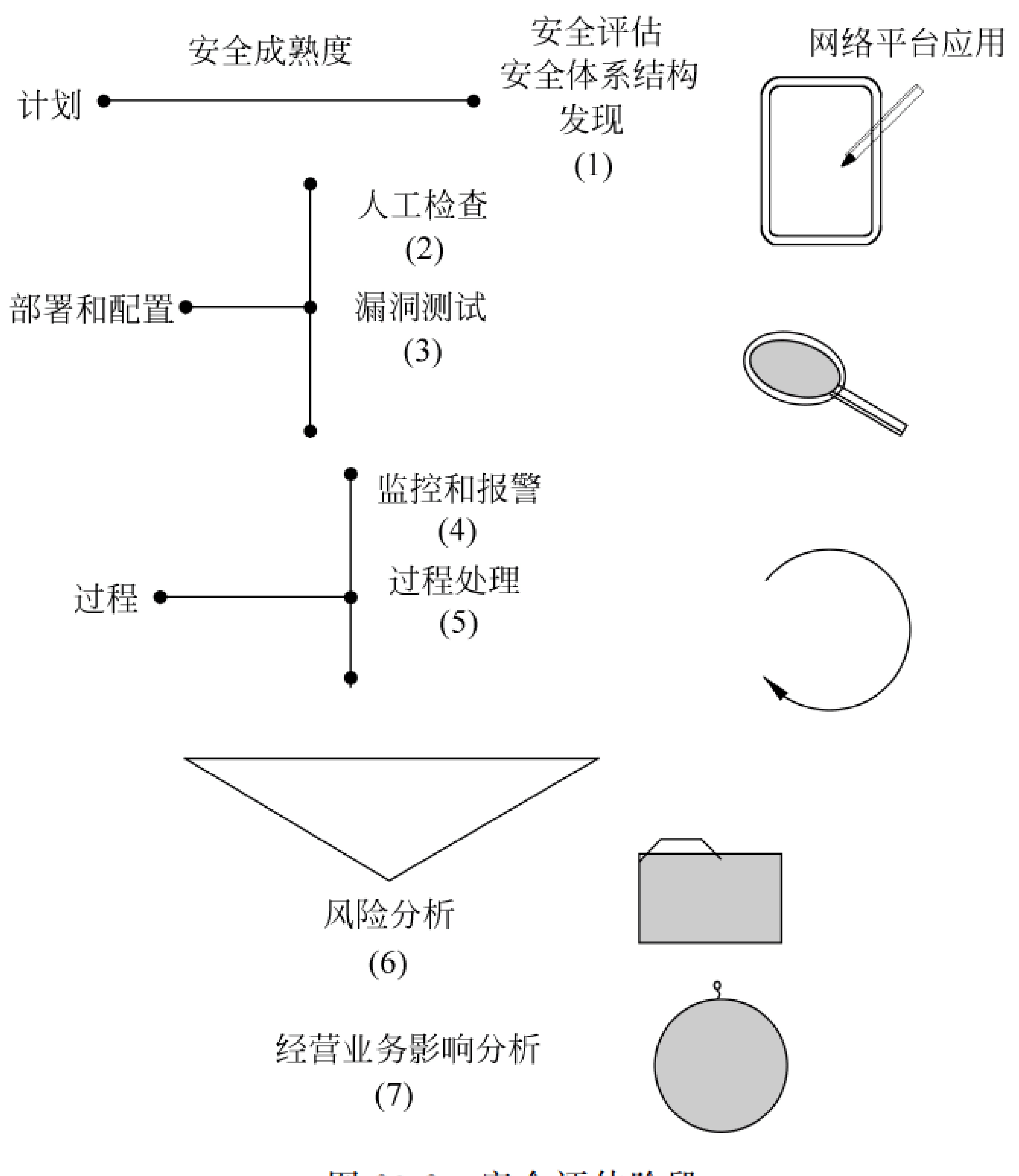


图 20-2　安全评估阶段

20.4.2　网络安全评估

由于 Internet 协议 TCP/IP 的实施没有任何内置的安全机制，因此大部分基于网络的应用也是不安全的。网络安全评估的目标是保证所有可能的网络安全漏洞是关闭的。多数网络安全评估是在公共访问的机器上，从 Internet 上的一个 IP 地址来执行的，诸如 E-mail 服务器、域名服务器(DNS)、Web 服务器、FTP 和 VPN 网关等。另一种不同的网络评估实施是给出网络拓扑、防火墙规则集和公共可用的服务器及其类型的清单。

网络评估的第 1 步是了解网络的拓扑。假如防火墙在阻断跟踪路由分组，这就比较复杂，因为跟踪路由器是用来绘制网络拓扑的。

第 2 步是获取公共访问机器的名字和 IP 地址，这是比较容易完成的。只要使用

DNS 并在 ARIN(American Registry for Internet Number)试注册所有的公共地址。

最后 1 步是对全部可达主机做端口扫描的处理。端口是用于 TCP/IP 和 UDP 网络中将一个端口标识到一个逻辑连接的术语。端口号标识端口的类型,例如 80 号端口专用于 HTTP 通信。假如给定端口有响应,那么将测试所有已知的漏洞。表 20-2 列出了各种类型的端口扫描技术。

表 20-2　端口扫描技术

端口扫描技术	描　　述
原型 TCP/IP 连接	打开一个连接观察感兴趣的端口并监听(在攻击的主机上不需专门的特权)。假如平台、防火墙或 IDS 正在监控该分组,则易于检测端口的扫描
TCP SYN(半开)	这个类型的扫描不是完全的 TCP 三次握手(SYN 输出,Ack 返回,Rst 输出)。在大多数情况下,监控不会捕捉它,但需要根据管理特权来控制低层联网数据
TCP FIN,Xmas 或 Null(偷袭)扫描	TCP 协议文本(RFC 793)规定关闭的端口必须对 reset(RST)分组响应。利用该特性能在无检测情况检测哪些端口是开启或关闭的。Microsoft 的联网栈不响应 RST 分组,这是另一种来识别网络上平台类型的方法
TCP FTP 代理(反弹攻击)扫描	这种技术可利用一个 FTP 服务器到代理(转发请求)的联接进入组织。换句话说,能使用位于防火墙后的一个 FTP 扫描在防火墙内的地址
TCP ACR 和 Windows 扫描	这个技术用于某些操作系统联网核心 TCP 窗口大小报告的异常
UDP 未处理 ICMP 端口不可达扫描	很多 UDP 服务(例如 SNMP、NFS、TFTP 和 DNS)运行在平台上。这个方法是对目标机的每个端口发送一个 0 字节的 UDP 分组。假如返回一个不可达 ICMP 端口,那么该端口是关闭的,否则假定端口是开启的
直接 RPC 扫描	这个技术用于所有打开的 TCP/UDP 端口,并用 Sun RPC 程序 NULL 命令将其扩散。假如 RPC 运行在任何端口,那么程序及版本号将发送到攻击的机器
由 TCP/IP 远程用户信息服务程序实现远程 OS 标识	内联网堆栈标识主机操作系统及版本

20.4.3　平台安全评估

平台安全评估的目的是认证平台的配置(操作系统对已知漏洞不易受损、文件保护及配置文件有适当的保护)。认证的唯一方法是在平台自身上执行一个程序。有时该程序称为代理,因为集中的管理程序由此开始。假如平台已经适当加固,那么有一个基准配置。评估的第 1 部分是认证基准配置、操作系统、网络服务(FTP、rlogin、telnet、SSH 等)没有变更。黑客首先是将这些文件替换成自己的版本。这些版本通常是记录管理员的口令,并转发给 Internet 上的攻击者。假如任何文件需打补丁或需要使用服务包,代理将通知管理员。

第 2 部分测试是认证管理员的口令,大部分机器不允许应用用户登录到平台,对应用的用户鉴别是在平台上运行的,而不是平台本身。

此外,还有测试本地口令的强度,如口令长度、口令组成、字典攻击等。

最后跟踪审计子系统,在黑客作案前就能跟踪其行迹。

数据库的安全评估也是必需的，这部分内容不在本书叙述范围内。

20.4.4 应用安全评估

应用安全评估比使用像网络和平台扫描这些自动工具而言，需要更多的技艺。黑客的目标是得到系统对应用平台的访问，强迫应用执行某些非授权用户的行为。很多基于Web应用的开发者使用公共网关接口(Common Gateway Interface，CGI)来分析表格，黑客能利用很多已知漏洞来访问使用 CGI 开发的 Web 服务器平台(例如放入“&”这些额外的字符)。

低质量编写的应用程序的最大风险是允许访问执行应用程序的平台。当一个应用损坏时，安全体系结构必须将黑客包含进平台。一旦一台在公共层的机器受损，就可用它来攻击其他的机器。最通用的方法是在受损的机器上安装一台口令探测器。

20.5 安全评估准则

根据计算机信息系统安全技术发展的要求，信息系统安全保护等级划分和评估的基本准则如下。

1. 可信计算机系统评估准则

TCSEC(Trusted Computer System Evaluation Criteria，可信计算机系统评估准则)是由美国国家计算机安全中心(NCSC)于 1983 年制定的计算机系统安全等级划分的基本准则，又称橘皮书。1987 年 NCSC 又发布了红皮书，即可信网络指南(Trusted Network Interpretation of the TCSEC，TNI)，1991 年又发布了可信数据库指南(Trusted Database Interpretation of the TCSEC，TDI)。

2. 信息技术安全评估准则

ITSEC(Information Technology Security Evaluation Criteria，信息技术安全评估准则)由欧洲四国(荷、法、英、德)于 1989 年联合提出，俗称白皮书。在吸收 TCSEC 的成功经验的基础上，首次在评估准则中提出了信息安全的保密性、完整性、可用性的概念，把可信计算机的概念提高到可信信息技术的高度。

3. 通用安全评估准则

CC(Command Criteria for IT Security Evaluation，通用安全评估准则)由美国国家标准技术研究所(NIST)、国家安全局(NSA)、欧洲的荷、法、德、英以及加拿大等 6 国 7 方联合提出，并于 1991 年宣布，1995 年发布正式文件。它的基础是欧洲的白皮书 ITSEC、美国的(包括橘皮书 TCSEC 在内的)新的联邦评价准则、加拿大的 CTCPEC 以及国际标准化组织的 ISO/SCITWGS 的安全评价标准。

4. 计算机信息系统安全保护等级划分准则

我国国家质量技术监督局于 1999 年发布的国家标准，序号为 GB17859—1999。评价

准则的出现为我们评价、开发、研究计算机及其网络系统的安全提供了指导准则。

20.5.1　可信计算机系统评估准则

TCSEC 共分为 4 类 7 级：D、C1、C2、B1、B2、B3、A1。

1. D 级

安全性能达不到 C1 级的划分为 D 级。D 级并非没有安全保护功能，只是太弱。

2. C1 级，自主安全保护级

可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制(如访问控制表)允许命名用户和用户组的身份规定并控制客体的共享，并阻止非授权用户读取敏感信息。

可信计算基(Trusted Computing Base，TCB)是指为实现计算机处理系统安全保护策略的各种安全保护机制的集合。

3. C2 级，受控存取保护级

与自主安全保护级相比，本级的可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件以及隔离资源，使用户能对自己的行为负责。

4. B1 级，标记安全保护级

本级的可信计算基具有受控存取保护级的所有功能。此外，还可提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述，具有准确地标记输出信息的能力，可消除通过测试发现的任何错误。

5. B2 级，结构化保护级

本级的可信计算基建立于一个明确定义的形式安全策略模型之上，它要求将 B1 级系统中的自主和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的可信计算基必须结构化为关键保护元素和非关键保护元素。可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的复审。加强了鉴别机制，支持系统管理员和操作员的职能，提供可信设施管理，增强了配置管理控制。系统具有相当的抗渗透能力。

6. B3 级，安全域级

本级的可信计算基满足访问监控器需求。访问监控器是指监控主体和客体之间授权访问关系的部件。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的，必须足够小，能够分析和测试。为了满足访问监控器需求，可信计算基在其构造时排除实施对安全策略来说并非必要的代码。在设计和实现时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

7. A1 级，验证设计级

本级的安全功能与 B3 级相同，但最明显的不同是本级必须对相同的设计运用数学

形式化证明方法加以验证，以证明安全功能的正确性。本级还规定了将安全计算机系统运送到现场安装所必须遵守的程序。

20.5.2　计算机信息系统安全保护等级划分准则

这是我国国家质量技术监督局于 1999 年发布的计算机信息系统安全保护等级划分的基本准则，是强制性的国家标准，序号为 GB17859—1999。准则规定了计算机信息系统安全保护能力的 5 个等级。

1. 概述

《准则》是计算机信息系统安全等级保护系列标准的核心，制定《准则》是实行计算机信息系统安全等级保护制度建设的重要基础，其主要目的是：

- 支持计算机信息系统安全法规的制定；
- 为计算机信息系统安全产品的研发提供功能框架；
- 为安全系统的建设和管理提供技术指导。

《准则》在系统地、科学地分析计算机处理系统的安全问题的基础上，结合我国信息系统建设的实际情况，将计算机信息系统的安全等级划分为如下 5 级：

- 第一级，用户自主保护级；
- 第二级，系统审计保护级；
- 第三级，安全标记保护级；
- 第四级，结构化保护级；
- 第五级，访问验证保护级。

各级的命名，主要考虑了使各级的名称能够体现这一级别安全功能的主要特性。计算机信息系统安全保护能力随着安全保护等级的增高，逐渐增强。5 个级别的安全保护能力之间的关系如图 20-3 所示。

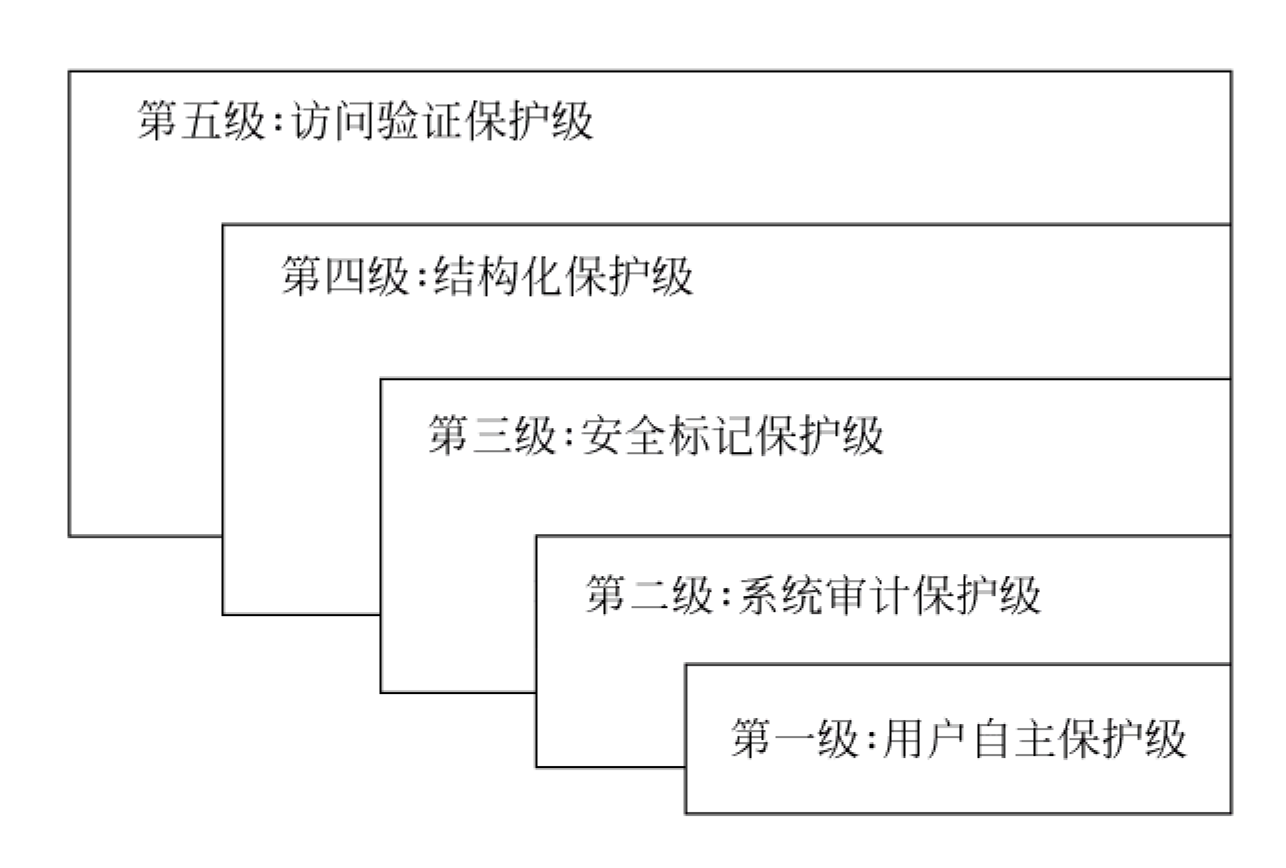


图 20-3　各等级安全保护能力示意图

2 技术功能说明

在计算机信息系统的安全保护中，一个重要的概念是可信计算基。可信计算基是一

个实现安全策略的机制，包括硬件、软件和必要的固件，它们将根据安全策略来处理主体（系统管理员、安全管理员和用户）对客体（进程、文件、记录、设备等）的访问。可信计算基具有以下特性：

- 实施主体对客体的安全访问的功能；
- 抗篡改的性质；
- 易于分析与测试的结构。

在《准则》规定的 5 个级别中，其安全保护能力主要取决于可信计算基的特性，即各级之间的差异主要体现在可信计算基的构造及它所具有的安全保护能力上。

20.5.3　通用安全评估准则

1. 概述

通用安全评估准则（CC）是一个国际标准。该标准描述了这么一个规则："……可作为评估 IT 产品与系统的基础……，这个标准允许在相互独立的不同安全评估结果之间进行比较……，提供一套公共的用于 IT 产品与系统的安全功能集，以及适应该功能集的安全保障的测度。评估过程确定了 IT 产品与系统关于安全功能及保障的可信水平"。CC 由 3 个部分组成：安全功能、安全保障与评估方法。信息系统安全工程（ISSE）可以利用 CC 作为工具支持其行为，包括为信息保护系统制定系统级的描述和支持批准过程。

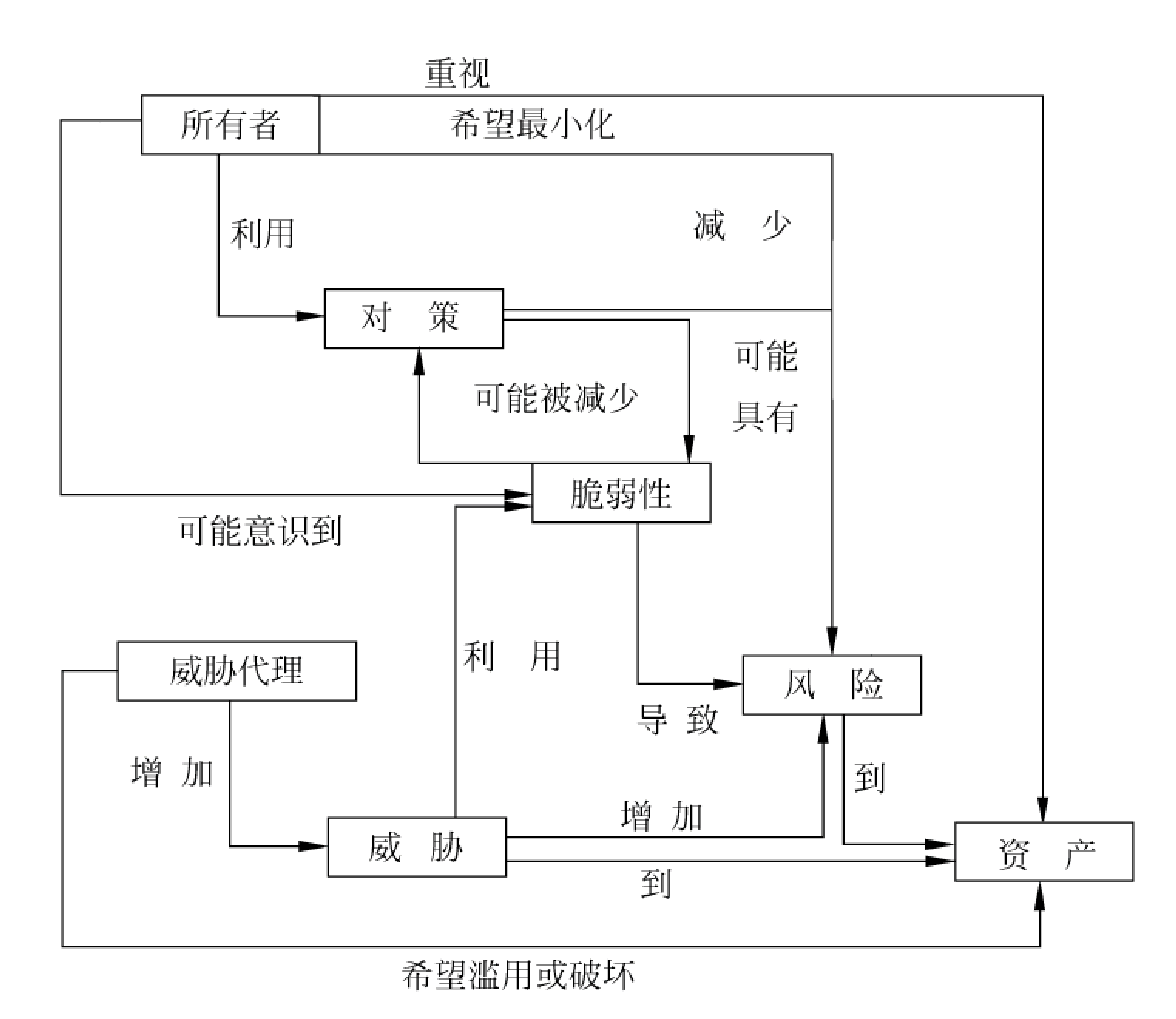


图 20-4　CC 中的安全概念与相互关系

图 20-4 显示 CC 是如何应用的，用 CC 的语法建立信息安全的过程是符合 ISSE 过程的。发掘信息保护需求的行为提供了各种信息，如所有者怎样评估资产、威胁代理是什么、什么是威胁、什么是对策（要求与功能）和什么是风险（部分地）。定义信息保护系统的行为提供了用于描述如下事务的信息：什么是对策（命名组件）、什么是脆弱性（基于体系

结构)、什么是风险(更全面)。设计信息保护系统的行为提供了如下信息：什么是对策(验证了的信息保护产品功能)、什么是脆弱性(基于设计的、组合并验证了的测试结果)和什么是风险(更加全面)。实现信息保护系统的行为最后提供了如下信息：什么是对策(安装了的、有效的信息系统保护功能)、什么是脆弱性(基于有效性与漏洞测试实现结果)、什么是风险(更加全面)。CC 并不描述个体和操作的安全,也不描述评估的有效性或其他使系统更有效的管理经验。CC 提供了一种标准的语言与语法,用户和开发者可以用它来声明系统的通用功能(保护轮廓或 PP)或被评估的特定性能(安全目标或 ST)。

PP 都以标准化的格式定义了一套功能要求与保障要求,它们或者来自于 CC,或由用户定义,用来解决已知的或假设的安全问题(可能定义成对被保护资产的威胁)。对于一个完全与安全目标一致的评估对象(TOE)集合,PP 允许各对象有独立的安全要求表述。PP 设计是可重用的,并且定义了可有效满足确定目标的 TOE 环境。PP 也包括了安全性与安全目标的基本依据。即使评估对象是特定类型的 IT 产品、系统(如操作系统、数据库管理系统、智能卡、防火墙等),其安全需求的定义也不会因系统不同而不同。

PP 可以由用户团体、IT 产品开发者或其他有兴趣定义这样一个需求集合的集体开发。PP 给了消费者一个参考特定安全需求集合的手段,并使得用户对这些要求的评估变得容易。因此,PP 是一个合适的用于 ISSE 开发并描述其架构的 CC 文档,可以作为查询与技术评估的基础。

ST 包括一个参考 PP 的安全需求的集合,或者直接引用 CC 的功能或保障部分,或是更加详细地对其说明。ST 使得对稳定 TOE 的安全需求的描述能够有效地满足确定目标的需要。ST 包括评估对象的概要说明、安全要求与目标及其根据。ST 是各团体对 TOE 所提供的安全性达成一致的基础。

PP 和 ST 也可以是在负责管理系统开发的团体、系统的核心成员及负责生产该系统的组织之间互相沟通的一种手段。在这种环境中,应该建议 ST 对 PP 做出响应。PP 与 ST 的内容可以在参与者之间协商。基于 PP 与 ST 的对实际系统的评估是验收过程的一部分。总的来说,非 IT 的安全需求也将被协商和评估。通常安全问题的解决并不是独立于系统的其他需求的。ST 与 PP 的关系如图 20-5 所示。

CC 的观点是,在对即将要信任的 IT 产品和系统进行评估的基础之上提供一种保障。评估是一种传统的提供保障的方式,同时也是先期评估准则文档的基础。为了与现有方式一致,CC 也采纳了同样的观点。CC 建议专业评估员加大评估的广度、深度与强度,来检测文档的有效性和 IT 产品或系统的结果。

CC 并不排除也不评估其他获取保障的方法的优点。针对其他可替代的获取保障的方法正在研究。这些研究行为所产生的可替代的方法可能会被考虑加入到 CC 之中,而 CC 的结构允许它今后引入其他方法。

CC 的观点宣称,用于评估的努力越多,安全保障效果越好;CC 的目标是用最小的努力来达到必需的保障水平。努力程度的增加基于如下因素：

- 范围,必须加强努力,因为大部分的 IT 产品与系统包含在内。
- 深度,努力必须加深,因为评估证据的搜集依赖于更好的设计水平与实现细节。
- 强度,努力必须加大,因为评估证据的搜集需要结构化和正式的方式。

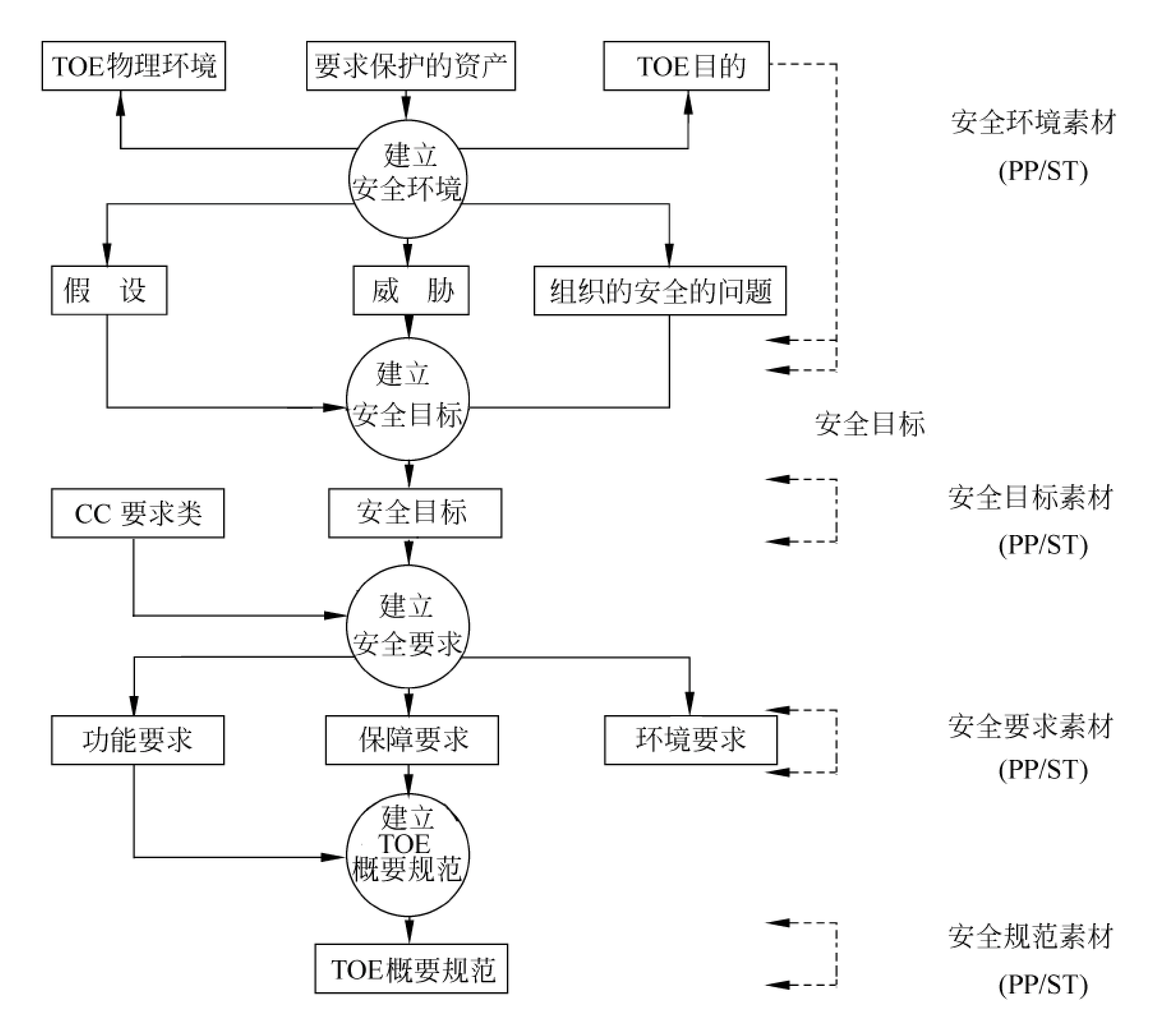


图 20-5　保护轮廓与安全目标的关系

- 评估过程为 PP 与 ST 所需的保障提供了证据，如图 20-6 所示。评估的结果就是对信息保护系统的某种程度上的确信。其他 ISSE 过程，如风险管理，提供了将这种确信转化成管理决策准则的方法。

图 20-7 说明了系统（或子系统）可以参照 PP 或 ST 得到评估，辅以外部认证与批准准则，从而创建评估产品集，以对系统的批准过程提供支持。

2 安全功能要求与安全保证要求

（1）安全功能要求

安全功能要求分为以下 11 类：

- 安全审计类；
- 通信类（主要是身份真实性和抗否认）；
- 密码支持类；
- 用户数据保护类；
- 标识和鉴别类；
- 安全管理类（与 TSF 有关的管理）；
- 隐秘类（保护用户隐私）；
- TSF 保护类（TOE 自身安全保护）；
- 资源利用类（从资源管理角度确保 TSF 安全）；

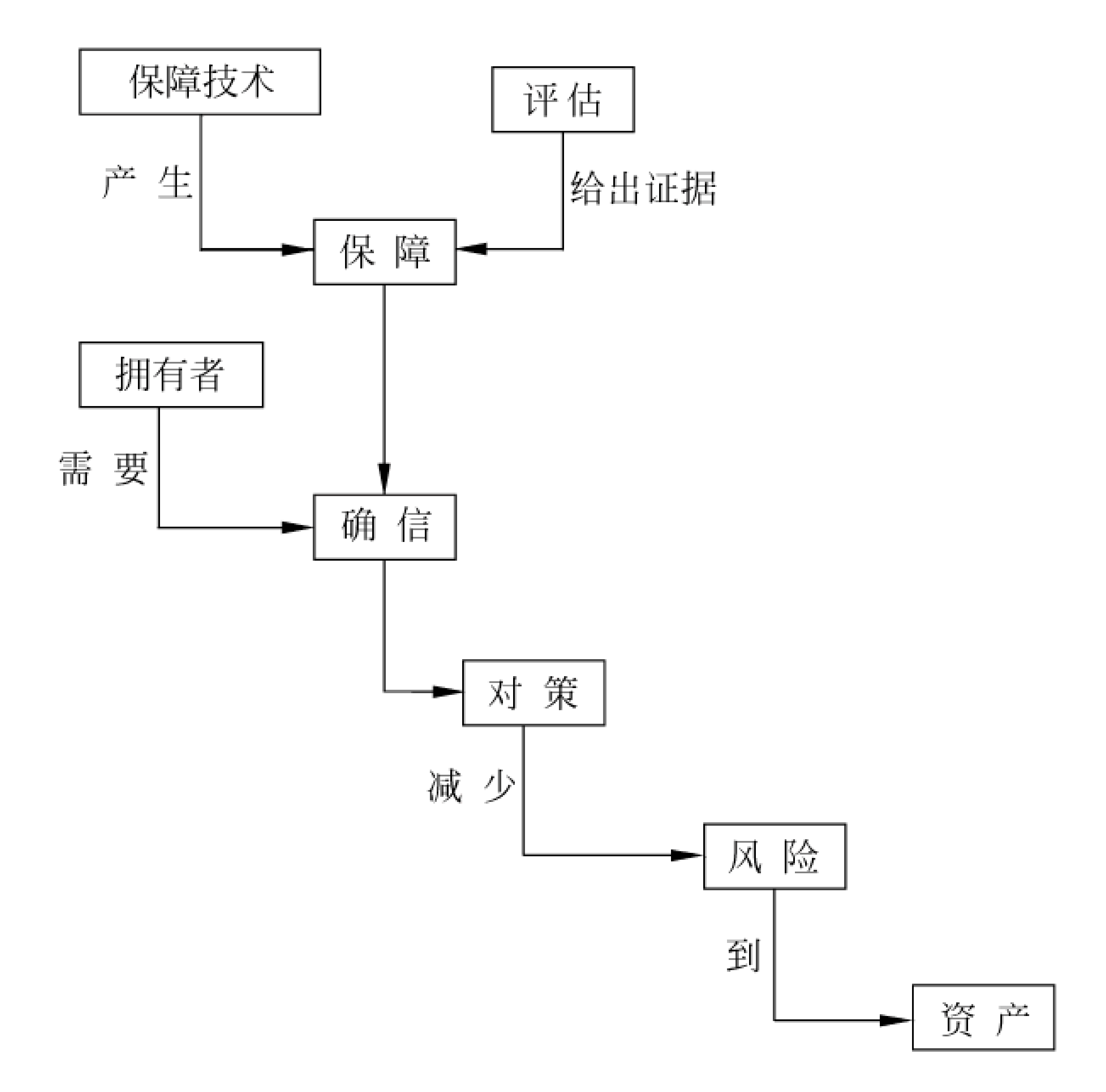


图 20-6　评估的概念与相互关系

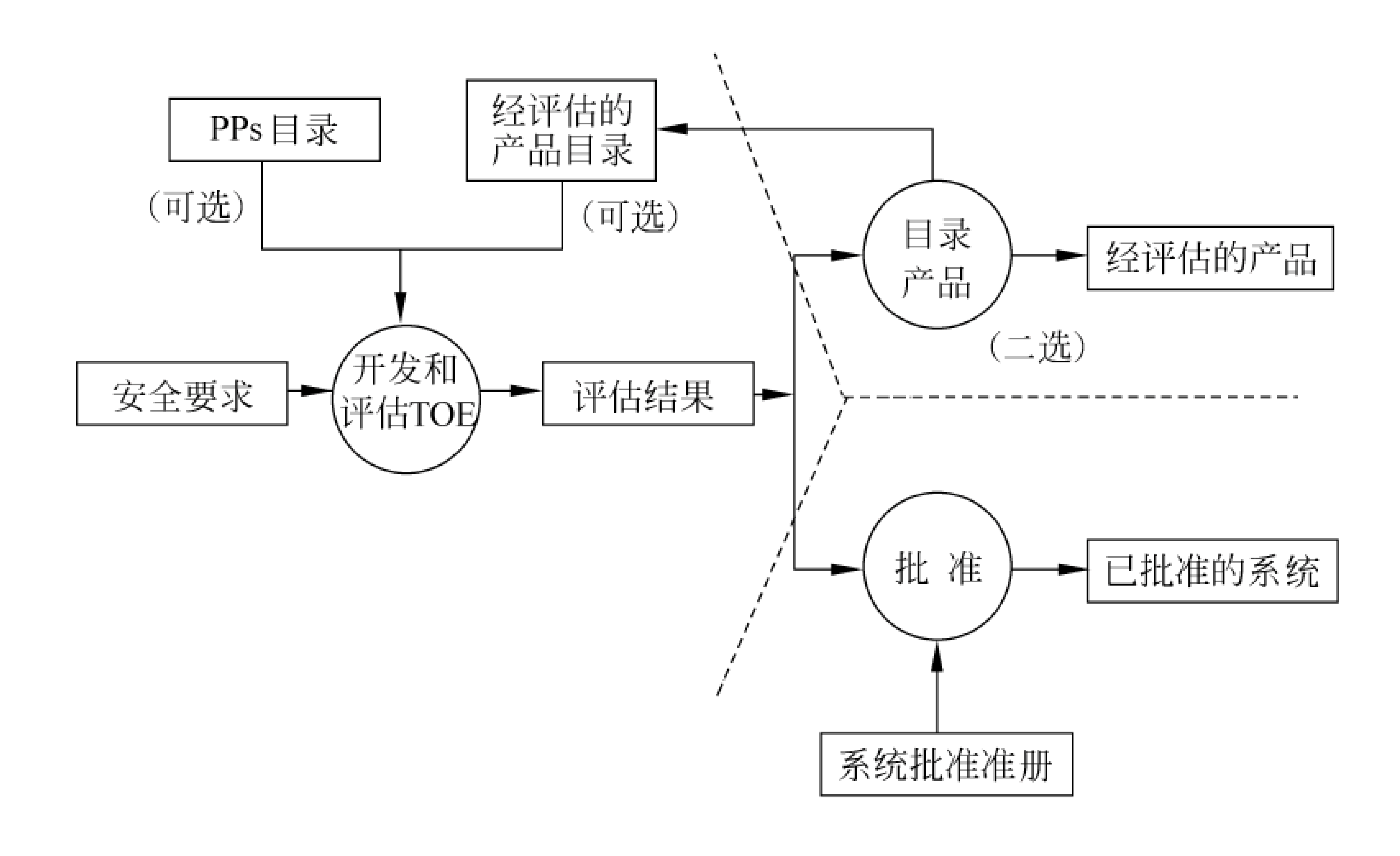


图 20-7　使用评估结果

- TOE 访问类(从对 TOE 的访问控制确保安全性);
- 可信路径/信道类。

这些安全类又分为族,族中又分为组件。组件是对具体安全要求的描述。从叙述上看,每一个族中的具体安全要求也是有差别的,但 CC 没有以这些差别作为划分安全等级的依据。

(2) 安全保证要求

在对安全保护框架和安全目标的评估进行说明以后,将具体的安全保证要求分为以下 8 类:

- 配置管理类；
- 分发和操作类；
- 开发类；
- 指导性文档类；
- 生命周期支持类；
- 测试类；
- 脆弱性评定类；
- 保证的维护类。

按照对上述 8 类安全保证要求的不断递增，CC 将 TOE 分为 7 个安全保证级，分别是：

- 第一级，功能测试级；
- 第二级，结构测试级；
- 第三级，系统测试和检查级；
- 第四级，系统设计、测试和复查级；
- 第五级，半形式化设计和测试级；
- 第六级，半形式化验证的设计和测试级；
- 第七级，形式化验证的设计和测试级。

20.6　本章小结

风险管理是识别、评估和减少风险的过程。风险评估对漏洞和威胁的可能性进行检查，并考虑事故造成的可能影响。描述威胁和漏洞最好的方法是根据对经营业务的影响来描述。

成熟度模型可用来测量组织的解决方案（软件、硬件、系统）的能力和效力，可用于安全评估方法，以测量针对业界最佳实际的安全体系结构。可以就以下 3 个方面进行分析：安全计划、技术和配置、操作运行过程。

弄清楚威胁的来源是减少威胁得逞可能性的关键。威胁源包括人为差错和设计缺陷、内部人员、临时员工、自然灾害和环境危害、黑客和其他入侵者、病毒和其他恶意软件。

威胁的情况包括系统管理过程、电子窃听、软件利用、信任转移、数据驱动攻击、拒绝服务、DNS 欺骗、源路由，以及内部威胁。应采取相应对策和保护措施。

安全评估可分 5 个阶段：①发现阶段，对安全体系结构及安全基础设施设计文本的检查；②人工检查阶段，将文本描述的体系结构和设计与实际的结构进行比较，找出差别；③漏洞测试阶段，包括网络、平台和应用的漏洞测试，平台扫描，应用扫描；④监控和报警；⑤安全体系结构的处理过程。在此基础上得出风险分析文本以及经营业务影响分析。

网络安全评估的目标是保证所有可能影响网络安全的利用是关闭的。评估的过程包括了解网络的拓扑、获取公共访问机器的名字及其 IP 地址、对全部可达主机做端口扫描

的处理。

根据计算机信息系统安全技术发展的要求，提出信息系统安全保护等级划分和评估的基本准则。可信计算机系统评估准则(TCSEC)是全世界第 1 个计算机系统安全等级划分的基本准则，又称橘皮书。通用安全评估准则(CC)是由西方 6 国 7 方联合提出的作为评估 IT 产品与系统的基础的一个国际标准。计算机信息系统安全保护等级划分准则 GB17859—1999 是我国首次制定的为评价、开发、研究计算机及网络系统的安全提供的指导准则。

习　题

1. 什么是风险管理？简述风险评估的方法。
2. 安全成熟度模型的作用是什么？应从哪些方面来分析？
3. 弄清楚威胁的来源是减少威胁得逞可能性的关键，哪些是主要的威胁源？
4. 什么是防止电子窃听的保护措施？
5. 什么是导致不安全的最常见的软件缺陷？
6. 简述从安全成熟度模型 3 个方面的安全评估阶段。
7. 简述网络安全评估的过程和方法。
8. 可信计算机系统评估准则的适用范围是什么？
9. 计算机信息系统安全保护等级划分准则是一个强制性的国家标准，制定该标准的主要目的是什么？安全等级是如何划分的？
10. 通用安全评估准则 CC 是一个国际标准，CC 由哪几部分组成？其主要内容是什么？

附　录

各章习题答案

第1章

1. C	2. D	3. D	4. C	5. A
6. B	7. C	8. A	9. A	10. C

第2章

1. B	2. D	3. B	4. A	5. C
6. A	7. D	8. D	9. E	10. C

第4章

1. D	2. C	3. C	4. B	5. B
6. C	7. A	8. D	9. D	10. A

第5章

1. C	2. B	3. A	4. A	5. C
6. A	7. B	8. D	9. B	10. A
11. A	12. D	13. B	14. E	15. D
16. B	17. D	18. D	19. B	20. C
21. D	22. C	23. B	24. C	25. C

第9章

1. A	2. B	3. B	4. A	5. D

第10章

1. C	2. A	3. D	4. C	5. A
6. C	7. A	8. A		

第11章

3. B

第14章

1. A—a、f、g、h;B—b、c、e;C—i;D—d、j

4. B、D、F、I;A、C;E、G、H

第16章

5. B

第17章

1. B	2. C	3. B	4. D	5. D

第18章

1. D	2. D	3. B	4. D	5. C
6. C	7. B	8. A	9. C	10. A

参 考 文 献

1. Eric Maiwald. Network Security. McGraw-Hill, 2001
2. Christopher M. King, Curtis E. Dalton & T. Ertem Osmanoglu. Security Architecture. McGraw-Hill, 2001
3. William Stallings. Network Security Essentials: Applications and Standards. Prentice-Hill, 2000
4. 胡道元. 网络设计师教程. 北京:清华大学出版社,2001
5. Douglas E. Comer. Internetworking with TCP/IP Vol I. Prentice-Hill, 2000
6. Information Assurance Technical Framework (IATF) Document 3.0. IATF Forum Webmaster, 2000
7. 信息处理系统开放系统互连基本参考模型——第二部分:安全体系结构(GB/T9387.2—1995)(等同于 ISO7498—2)
8. 计算机信息系统安全保护等级划分准则(GB17859—1999). 国家质量技术监督局发布,1999
9. Bruce Schneier. Digital Security in a Networked World. John Wiley & Sons, Inc., 2000
10. D. Brent Chapman, Elizabeth D. Zwicky. Building Internet Firewalls. O'Reilly & Associates, Inc., 1995
11. Marcus Goncalves . Firewalls: A Complete Guide, 2000
12. William R. Cheswick, Steven M. Bellovin. Firewalls and Internet Security, 2000
13. The Twenty Most Critical Internet Security Vulnerabilities (http://www.sans.org/top20/)
14. Casey Wilson, Peter Doak. Creating and Implementing Virtual Private Networks. The Coriolis Group,1999
15. Naganand Doraswamy, Dan Harkins. IPSec: The New Security Standard for the Internet, Intranets and Virtual Private Networks. Prentice Hall,1999
16. Bruse Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C, Second Edition, John Wiley and Sons, 1995
17. Steve Burnett and Stephen Paine. RSA Security's Official Guide to Cryptography. Osborne McGraw-Hill, 2001
18. Stuart McClure, Joel Scambray, George kurtz. Hacking Exposed: Nertwork Security Secrets & Solutions. McGraw-Hill, 2001
19. Matt Bishop. Vulnerabilities Analysis, 1999
20. Rick Tims. Social Engineering: Policies and Education a Must, February 16, 2001
21. Dan Farmer, Wietse Venema. Improving the Security of Your Site by Breaking into it, 1993
22. Ofir Arkin. Network Scanning Techniques, Nov., 1999
23. Matt Bishop, David Bailey. A Critical Analysis of Vulnerability Taxonomies, 1996
24. Dennis Longley and Michael Shain. The Data & Computer Dictionary of Standards, Concepts and Terms, 1990
25. 薛静锋. UNIX 主机安全漏洞分析及漏洞扫描器的设计与实现, 2002
26. Rebecca Bace. An Introduction to Intrusion Detection and Assessment
27. Mike Fiskyx, George Varghesey. Fast Content-Based Packet Handling for Intrusion Detection. UCSD Technical Report CS2001-0670, May, 2001
28. Mark Crosbie. Automated Intrusion and Misuse Detection: A Guide to Understanding the

Technology and Evaluating Your Needs
29. Martin Roesch. Snort Users Manual, 10th August, 2001
30. Michael Mullins. Implementing a Network Intrusion Detection System, 16 May, 2002
31. 胡道元. Intranet 网络技术及应用. 北京：清华大学出版社，1998
32. David Harley, Robert Slade, Urs E. Cattiker. Viruses Revealed. McGraw-Hill, 2001
33. 戴宗坤、罗万伯等.信息系统安全.北京：电子工业出版社，2002
34. 闵京华.电子政务中的应用安全平台.《信息安全与通信保密》,2002第9期(总21期),第41页
35. ISO/IEC 17799: 2000 Information Technology-Code of Practice for Information Security Management
36. BS7799-2: 1999 Information Security Management-Specification for Information Security Management Systems
37. 信息系统安全技术国家标准汇编.北京：中国标准出版社，2000
38. Neal Krawetz. Introduction to Network Security. Charles River Media, 2007
39. Information Systems Security Certification Consortium Certified Information Systems Security Professional, 2006
40. ISO/IEC FDIS 18028-2:2005 Information technology-Security techniques-IT Network security-Part 2: Network security architecture
41. Jeff Shawgo the Center for Internet Security http: //www. cisecurity. org windows 2000 Server benckmark level-2 November 15, 2004
42. http: //www. sans. org SANS Top-20 Internet Security Attack Targets (2006 Annual Update)
43. ISO/IEC FDIS 18028-1:2006 Information technology-Security techniques-IT Network security-Part 1: Network security management
44. ISO/IEC 17799:2005 Information technology-Security techniques-Code of practice for information security management
45. ISO/IEC 27001: 2005 Information technology-Security techniques-Information security management systems-Requirements

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室　　计算机与信息分社营销室 收

邮编：100084　　电子邮件：jsjjc@tup.tsinghua.edu.cn

电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：网络安全（第 2 版）

ISBN：978-7-302-17963-4

个人资料

姓名：________________ 年龄：_______ 所在院校/专业：_____________________

文化程度：____________ 通信地址：_______________________________________

联系电话：____________ 电子信箱：_______________________________________

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议_______________________________

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议_______________________________

您对本书的总体满意度：

从语言质量角度看 □很满意 □满意 □一般 □不满意

从科技含量角度看 □很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？（可附页）

____

____

您希望本书在哪些方面进行改进？（可附页）

____

____

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页（http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn）上查询。